SECURITY TESTING RULES OF ENGAGEMENT

Last Updated: 2024-11-06

This Security Testing Rule of Engagement forms part of the *Master Professional Services Agreement* ("Principal Agreement") between: (i) for US based "Client": **ABACUS INFORMATION TECHNOLOGY, LLC (d/b/a Abacus Group LLC)**; or for UK based "Client": **ABACUS INFORMATION TECHNOLOGY UK LIMITED** (*collectively* "**Abacus**") acting on its own behalf and as agent for each Abacus Affiliate; and (ii) "**CLIENT"** *(as detailed in the respective Principal Agreement)* acting on its own behalf and as agent for each Client Affiliate.

The terms used herein shall have the meanings as set forth herein. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Principal Agreement. Except where the context requires otherwise, references herein to the Principal Agreement are to the Principal Agreement as amended by, and including, this addendum.

This Security Testing Rule of Engagement (this *"Policy"*), effective as of the Effective Date, governs Client's use of Abacus's Products and Services. Client agrees that it is responsible for ensuring that all of its Authorized Users comply with this Policy. Capitalized terms used herein and not otherwise defined herein have the meanings ascribed to such terms elsewhere in the Principal Agreement.

1. Purpose: To outline the scope, objectives, and constraints of the security testing engagement between Abacus and Client.

2. Scope: Client is authorizing Abacus to perform security testing on the systems defined in the applicable SOW(s). Abacus will have timely access to the relevant prerequisites listed within the proposed services.

3. Objectives: The objectives of the security testing engagement are to identify and assess vulnerabilities in the systems, network segments, and/or applications within the scope of the engagement. In the circumstances that penetration testing or social engineering is within the scope of authorized services, exploitation of vulnerabilities will be performed. Where exploitation is performed, Abacus will take the utmost precaution not to disrupt the confidentiality, integrity, and availability of all systems within the security testing scope.

4. Constraints: The constraints of the engagement include, but are not limited to:
    - Abacus will not perform any activity that is likely to cause harm to Client's systems, network segments, or applications.
    - Abacus will not access any systems, network segments, or applications outside of the scope of the engagement without prior written consent from Client. Security testing findings are strictly limited to the defined scope of systems.
    - Abacus will not perform any activity that is illegal or unethical, and will comply with all applicable laws and regulations pertaining to information security.

- Abacus's security testing is timebound within the mutually agreed timeframe. Real malicious actors are not timebound; therefore, Abacus cannot warrant the discovery of any security findings that may take an inordinate amount of time to reverse engineer or discover.
- When performing security testing engagements like penetration testing; Abacus emulates the capabilities of a sophisticated malicious actor but does not have the resources to emulate a state-level malicious actor. This considered, Abacus does not warrant the discovery of any zero-day vulnerabilities or exploits.

5. Qualifications**:** Abacus warrants that all staff participating in this security testing engagement are full-time staff of Abacus, who have undergone rigorous background checks as well as who possess cybersecurity expertise and qualifications.

6. Communication**:** Abacus and Client will agree upon a primary point of contact for each organization for the duration of the engagement. Abacus's cybersecurity services coordinator, defined within the "Roles and Responsibilities" section of this document, will be the person responsible for communication regarding the status and results of the engagement. Security testing status updates will be provided by Abacus on at least a weekly basis. Where high-severity security findings are identified on systems within the security testing scope, Abacus will communicate those findings as soon as possible to Client's defined point of contact. Client's point of contact will be defined shortly after signing this document.

7. Security Testing Timeframe**:** The start and end date of the engagement will be detailed in the applicable SOW(s) agreed upon by Abacus and Client prior to the start of the engagement. Security testing will be conducted on a 24x7 basis unless Client specifies otherwise. Abacus and Client may mutually agree to adjust the security testing timeframe as needed to ensure thorough analysis can be performed.

8. Employed Security Testing Standards**:** Security testing will be in alignment with PTES, MITRE ATT&CK, and NIST SP800-115 standards. Where web, mobile, serverless, and API applications are identified, OWASP Web Top Ten, OWASP Mobile Top Ten, OWASP Serverless Top Ten, and OWASP API Top Ten guidelines will be incorporated into the security testing process.

9. Abacus's Security Testing External IP Addresses**:** All security testing conducted by Abacus will originate from below subnets:

    - 20.62.182.160/28
    - 13.64.141.96/28
    - 20.121.232.64/28

    Note: These subnets should not be allow-listed in any system; it is merely to allow our customers to distinguish the difference between Abacus's security testing activities and potentially malicious activities from other sources.

10. Data Exfiltration**:** Abacus will not exfiltrate any sensitive company data that may be discovered in the course of the engagement, such as PHI (HIPAA), Sensitive PII, ABA/Bank Account Numbers, PAN (PCI-DSS Data), or Sensitive Company IP.

11. Deliverables**:** The deliverables for the engagement will include, as a minimum, a report detailing the security testing results, including a description of identified security findings, recommendations for remediation, and verification of remediation efforts.

12. Confidentiality**:** Abacus and Client agree to maintain the confidentiality of all information related to the engagement. Abacus will not disclose any sensitive data related to Client information systems collected from this security testing engagement to any unauthorized third parties. Abacus will encrypt all security testing data both in transit and rest with at least AES128 and TLS 1.2 or greater encryption algorithms throughout this information security engagement.

13. Termination**:** In the event of termination, Abacus will provide a summary report of the results of the engagement to Client.