MARCO'S TECHNOLOGY & SECURITY ASSESSMENTS AGREEMENT

This Technology Assessment, Cyber Security Assessment, and Basic Security Risk Assessment (collectively, "Assessment(s)") Agreement ("Assessment Agreement") is entered into by and between Marco Technologies, LLC with a principal place of business at 4510 Heatherwood Road, St. Cloud, MN ("Marco") and the legal entity identified in any Schedule of Products ("Client") (individually, "party," and collectively, "parties") for the Assessment(s) and services ("Services") that Client will purchase through or from Marco (collectively, "Products"). Client's purchase of and Marco's provision of the Products is subject to the Marco Relationship Agreement ("Agreement"). By its signature, electronic or otherwise, to any Schedule of Products ("SOP") for such Products, Client accepts and agrees that it is bound by the Agreement and this Assessment Agreement.

Assessments

Technology Assessment
Marco's Technology Assessment is designed to assist Client in identifying certain risks to Client's network and other information technology. The Technology Assessment includes Marco's review of a limited set of risks in eleven areas to the extent described below.

Marco will gather information for the Technology Assessment by conducting interviews with Client personnel, conducting an onsite visit at the site(s) designated on this document and deploying an IT assessment software tool. Client consents to providing Marco access to its network and other information technology for purposes of conducting the Technology Assessment as described on Schedule A which is attached hereto and incorporated herein by reference.

Marco will provide a summary of its findings in a presentation that identifies its primary concerns, the potential business impact of those concerns, and its remediation recommendation(s). Upon request, Marco will provide Client with the technical report produced by the IT assessment software tool which contains the complete findings from that tool.

Client understands and agrees that the Technology Assessment is not intended to be a comprehensive review of Client's network and information technology and is not a replacement for any legal compliance review or regulatory audit. If Client has specific concerns that it would like Marco to address about its network or other information technology, Client agrees to disclose those concerns prior to Marco's commencement of the Technology Assessment. The parties will then determine whether such concerns will be included in the Technology Assessment.

To develop recommendations, the following risk areas will be considered:

1. Power and Environment - Identifying certain defined exposures that may make equipment more susceptible to failure, delay technical issue resolution, or expose the organization to "drive by" attacks on physical equipment.

2. Server Infrastructure – Identifying certain lapses in specific best practices, aging systems that may impact function and performance, and opportunities to optimize and reduce risk of obsolescence.

© MARCO. ALL RIGHTS RESERVED.

3. Workstations – Identifying certain lapses in specific best practices, aging systems that may impact function and performance, and device identification standards.

4. Internet Infrastructure – Reviewing specific areas where procured services being rendered are not aligned with organizational needs as well as potential risk due to single point of failure or lack of visibility into failures when they occur.

5. Firewall– Reviewing device redundancy, the state of operating system code, availability and appropriate use of certain software capabilities that reduce the possibility of malware or malicious attacks while minimizing the inappropriate use of the internet by end-users and/or the potential for loss of connectivity due to hardware failure.

6. File Systems–Examining file system configurations for certain settings and missing functionality that could help avoid inappropriate, internal access to sensitive company information or challenges in efficiently recovering data or files in the case of common situation like accidental file deletion or server failures.

7. Email Systems –Assessing certain client/end-user access capabilities and ability to manage the current platform, evaluating use of a service to help prevent high volume of unwanted mail as well as virus and malware attacks, plus reviewing Exchange version details to gage stability and upgrade recommendations.

8. Applications– Evaluating version stability for certain applications and determining gaps in certain application best practices that potentially lead to extra time and cost when applications are installed and/or lack of control over employees' software use, licensing, and deployment.

9. Backup and Disaster Recovery– Reviewing a limited set of practices and functions to establish baseline risks that could result in loss of data and business productivity or delays in return back to business functionality following an unforeseen event.

10. Wireless Network – Discovering current configuration and management setting to identify certain gaps in the system or structure that result in limited connectivity or unintended user access to network.

11. Security Best Practices – Assessing whether client is adhering to a limited set of common security best practice measures. Adherence to these measures may help limit risk of systems, data, and access being compromised.

Basic Risk Security Assessment

The Basic Risk Security Assessment is designed to assist Client in identifying certain security risks to Client's business information. The Basic Risk Security Assessment includes Marco's review of a limited set of security risks in areas aligned with the National Institute of Standards and Technology, Cybersecurity Framework 1.1 April 2018 as described below.

Marco will gather information for the Basic Risk Security Assessments by conducting interviews with Client personnel.

Marco will provide a summary of its findings in a report that identifies its primary concerns, the potential business impact of those concerns, and its remediation recommendation(s).

© MARCO. ALL RIGHTS RESERVED.

Client understands and agrees that the Basic Risk Security Assessment is not intended to be a comprehensive information security review and is not a replacement for any legal compliance review, forensic review, general third party technology audit or regulatory audit.

To develop recommendations, the following risk areas will be considered:

1. Identify- Are you identifying and controlling who has access to your business information?
2. Protect- Are you protecting the confidentiality, integrity and availability of your business information?
3. Detect- Are you able to detect risks to your business information?
4. Respond- Are you able to respond to a disaster or an information security incident?
5. Recover- Are you prepared to recover from a disaster or an information security incident?

Cyber Security Assessment
Marco's Cyber Security Assessment is designed to assist Client in identifying certain risks to Client's network, business information, and other information technology. The Cyber Security Assessment includes all components of the Basic Risk Security Assessment defined above.

Additionally, Marco will provide the following network and information security review or testing as a part of its Cyber Security Assessment.

1. Review of Physical Security Controls. These controls may include facilities, computer rooms, media filing and storage, information systems offices, and telecommunications rooms.

2. Review of Logical Security Controls. These controls may include computer operating systems, computer applications, electronically stored files and libraries, and telecommunications software.

3. Social Engineering Testing Procedures. These procedures may include random contacting of Client personnel and agents for the purposes of obtaining private information, and random conduct of human engineering tests at facilities.

4. Electronic Network Scanning and Testing. These procedures may include use of software tools and techniques to gain information about external and/or internal network connections and devices connected to those networks, and the use of tools and techniques to test external and/or internal network connections and devices connected to those networks.

Any additional testing requested by Client or recommended by Marco will be subject to a Change Order.

Scope of Services

Marco has the right to determine the method, details, and means of performing the Assessments(s). Client has the right propose modifications to and stop Assessment(s).

© MARCO. ALL RIGHTS RESERVED.

Miscellaneous

Client shall pay the prices ("Price(s)") listed on the SOP for the Assessment(s). Client and Marco shall select a date to deliver final results of these Assessment(s) within six weeks from the signing of this document ("Presentation Date"). Marco shall invoice Client on the scheduled Presentation Date(s) and any Client delay in Presentation Date(s) shall not delay this billing.

Taxes, shipping, handling and other fees may apply where applicable. Marco reserves the right to cancel orders arising from pricing or other errors.

Authorization to Conduct Procedures

Client desires that Marco perform Assessment(s) of Client's computer system and network (including network and information security and vulnerability testing procedures) and expressly consents to and instructs Marco to perform such Assessment(s) by its acceptance of any Marco SOP for such Products. Marco's conduct of the Assessment(s), including network and information security and vulnerability testing services, may cause temporary interruptions or disabling of information processing capabilities. Client understands and accepts the risk of such interruption and disabling.

Client hereby authorizes Marco during its network and information security and vulnerability testing procedures to attempt to break into computer systems, and consents to Marco's use of penetrating techniques and strategies to attack existing security systems.

Client shall comply with all applicable laws, regulations and statutes relating to authorization and instructions to Marco to perform the Services. In the event that one or more IP addresses specified by Client identifies computer systems that are not owned by Client, including, but not limited to, firewalls, routers, and Web servers, Client agrees to:

- Obtain a letter that is reasonably satisfactory to Marco, signed by an authorized officer of the organization, from the owner of each computer system, indicating the owner's acceptance of the conditions set forth in this Assessment Agreement. Client also agrees to provide Marco with a copy of such authorization. If authorization by the systems' owner is not provided, these systems and devices will be excluded from Marco testing and related processes and procedures.
- Be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these computer systems by Marco network and information security and vulnerability testing services to the system owner, and for ensuring that the system owner takes all appropriate actions.
- Facilitate the exchange of information between the system owner and the Marco project team, as necessary.

Client agrees to inform Marco immediately, during the conduct of network and information security and vulnerability testing services, whenever there is a change in ownership of any system identified by the IP addresses communicated to Marco.

© MARCO. ALL RIGHTS RESERVED.

Acceptance of Limitations and Risk

Marco shall not be liable for any delays or failures in performance due to circumstances beyond its reasonable control.

Marco will take reasonable precautions to avoid causing one or more devices to become inoperative and result in loss of service or data. However, Marco cannot accurately predict those devices that could be adversely affected by its network and information security and vulnerability testing methods. Therefore, Client understands and accepts the risk that Marco performance of the Services may cause one or more devices to become inoperative and result in loss of service or data.

Version Effective Date: February 9, 2021

© MARCO. ALL RIGHTS RESERVED.