MARCO'S TECHNOLOGY & SECURITY ASSESSMENT AGREEMENT

This Technology Assessment and Information Security Assessment 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 order ("Client") (individually, "party," and collectively, "parties"). This is subject to and governed by the Relationship Agreement between the parties. If Client does not accept and comply with this Assessment Agreement, it may not place an order or use the 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.

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.

Information Security Assessment

The Information Security Assessment is designed to assist Client in identifying certain security risks to Client's business information. The Information 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 Information Security Assessment 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).

Client understands and agrees that the Information 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?

Miscellaneous

Client shall pay the prices ("Price(s)") listed on Schedule B hereto containing Marco's Schedule of Products for the Technology Assessment and the Information Security Assessment. Client and Marco shall select a date to deliver final results of these assessments 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. We reserve the right to cancel orders arising from pricing or other errors.

Effective: September 24, 2019