INFORMATION SECURITY ADDENDUM

This Information Security Addendum ("Addendum") forms part of the agreement that references and incorporates this Addendum ("Agreement") entered into between the Pavion Corp. or its affiliates ("Pavion") and the Subscriber specified in the Agreement ("Subscriber"). Notwithstanding any terms contained in the Agreement to the contrary, in the event of a conflict between the terms of the Agreement and the terms of this Addendum, the terms of this Addendum shall supersede and prevail.

1. **Scope and Applicability**. This document summarizes Pavion's information security controls and practices designed to protect the confidentiality, integrity, and availability of Subscriber's Confidential Information. Pavion is not the manufacturer or developer ("OEM") of certain products ("Third-Party Products") delivered or serviced by Pavion, and such OEMs are not Pavion subprocessors. Accordingly, Pavion does not control and is not responsible for the information security of Third-Party Products, except to the extent of processing performed directly by Pavion or its subcontractors. Subscriber remains responsible for maintaining the security of its own systems and environments, including those that interact with or are accessed by Pavion in connection with the services.

2. **Policies**. Pavion maintains written information security policies and procedures designed to protect Subscriber Information (defined below) from unauthorized access, use, disclosure, alteration, or destruction. These policies are reviewed and updated annually to address evolving security risks. Pavion maintains a dedicated information security team responsible for overseeing security governance, policy enforcement, risk management, and incident response across its operations, and this team reports regularly to executive leadership on information security risks, controls, and program effectiveness. "Subscriber Information" means non-public data or information provided by or on behalf of Subscriber in connection with Pavion's services, including business, operations, financial, personally identifiable, and other proprietary or sensitive information. Pavion maintains an Information Security Program designed to protect confidentiality, integrity, availability, and security of Subscriber Information that includes the following measures.

3. **Security Training**. Pavion provides information security training to its personnel at the time of hiring and annually thereafter. In addition, Pavion delivers ongoing security awareness through ad hoc and role-based training, including periodic phishing simulations, reminders, and other on-the-job reinforcement.

4. **Network Security**. Pavion utilizes real-time malware detection, managed detection and response (MDR) for suspicious activity alerts, network segmentation, and firewalls for intrusion detection and prevention. Additionally, Pavion centrally tracks and analyzes security analytics to identify risks using a security information and event management system (SIEM) and has DDoS protection on its public web servers. Critical security threats are relayed to Pavion's network security team immediately for disposition. Log data is retained for 12 months.

5. **Information Access**. Access to Subscriber Information is limited to employees, agents or subprocessors necessary for Pavion to perform under the Agreement. Subscriber Information is logically separated from information of other Subscribers.

6. **Destruction of Materials**. Pavion follows secure erasure and destruction procedures for electronic media and paper shredding measures in accordance with industry standards.

7. **Incident Response**. Pavion maintains incident response plans and procedures, conducts "tabletop" exercises annually, and regularly reports to executive leadership regarding information security posture and risk management efforts. Pavion has a dedicated Cyber Security team on call to handle critical system events. Pavion's documented Incident Response Plan identifies key stakeholders responsible for handling the response to a security incident should one occur. Pavion updates the plan to address newly identified risks or legal and regulatory requirements. Pavion's plan calls for timely Subscriber notifications and coordination with various internal stakeholders and outside resources to manage and resolve security incidents.

8. **Endpoint Security**. Pavion implements a layered endpoint security program across all end-user devices. Endpoints are protected with anti-virus and anti-malware software with real-time detection and automatic updates based on global threat intelligence. Pavion personal computers are full disk encrypted, password/PIN protected, and configured for automatic security patching. Devices are uniquely assigned to individual users, monitored for compliance with security policies, and restricted from running prohibited software.

9. **Vulnerability Testing**. Pavion performs periodic internal and external vulnerability assessments, application penetration tests, and annual external application and network penetration tests.

10. **Backup and Disaster Recovery**. Pavion's business applications are backed up periodically. Pavion maintains a business continuity and disaster recovery policy with specified RPOs and RTOs, geo-zone redundancy, standard recovery capabilities, designated personnel, and recovery procedures for key applications.

11. **Remote Access and Data Transfer**. Subscriber expressly authorizes Pavion and its designated third-party service providers to remotely access Subscriber's systems, networks, equipment, devices, and related interfaces as reasonably necessary to provide technical support, inspection, maintenance, troubleshooting, monitoring, and related services under this Agreement, including installation of software on Subscriber's systems that may transfer data to Pavion limited to system status updates and information, and shall obtain any third-party consents for such access and installation (as applicable). Subscriber shall defend, indemnify, and hold them harmless from any third-party claims, losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising from such authorized remote access, except to the extent finally determined to have been caused by Pavion's sole gross negligence or willful misconduct.