Security Exhibit

Effective Date: November 1, 2024

This Security Exhibit ("**Security Exhibit**") is incorporated into the executed Agreement between SMA Technologies and Customer, SMA Technologies' performance of the services must be in accordance with the Agreement and this Security Exhibit. Terms used here but not defined here are defined in the Agreement.

SMA Technologies reserves the right to periodically modify this Security Exhibit to reflect current security practices, and such modification will automatically become effective in the next Service Term.

Purpose. This Security Exhibit applies when SMA Technologies provides the Services and Support to Customer. SMA Technologies will make commercially reasonable efforts to prevent loss, theft, or damage to Customer Data from the Services. This Exhibit establishes the requirements necessary to maintain a security program and ensure that sufficient physical, operational, and technical security measures are in place for the protection of Customer Data in the Services.

1. Information Security Management

1.1 Information Security Management System. SMA Technologies maintains and continually makes improvements to a documented information security management system in accordance with industry-standard practices and accepted frameworks for the delivery of OpCon Services and Support which its personnel are to be made aware of and comply with ("Information Security Management System").

1.2 Certification. During the term of the Agreement, SMA Technologies shall maintain its AICPA SOC2 Type I report or equivalent as well as maintain a lawful transfer mechanism for export of personal data out of the European Union.

1.3 Testing. SMA Technologies conducts at least annual third-party penetration and vulnerability tests on applications and infrastructure used to support the provision of Services and Support to identify security vulnerabilities. SMA Technologies also conducts weekly SAST and DAST scans as part of our development lifecycle to identify vulnerabilities.

2. Organizational Security

2.1 Information Security Responsibilities. SMA Technologies has dedicated roles with clearly defined responsibilities for the administration of the Information Security Management System.

2.2 Security Policies. As part of the administration of the Information Security Management System, SMA Technologies has created information security policies that define responsibility for the protection of its systems and Customer Data ("Information Security Policies"). Information Security Policies include requirements designed to monitor compliance with privacy and information security policies and procedures.

3. Asset Classification

3.1 Asset Management. SMA Technologies maintains an asset management policy in accordance with industry-standard practices, including asset classification (*e.g.* information, software, hardware) and an inventory of devices and systems that administer the Services and Support to enable SMA Technologies to protect Customer Data and assets.

3.2 Asset Controls. SMA Technologies has established physical, organizational, and technical security controls to protect Customer Data from unauthorized access and disclosure.

4. People Security

4.1 SMA Technologies' Employees. SMA Technologies' employees and contract workers (collectively "Staff") must behave consistently with this Security Exhibit to ensure effective security. SMA Technologies makes its Staff aware of their responsibilities for maintaining effective security controls, particularly regarding the use of passwords, disposal of information, social engineering attacks, incident reporting, and the physical and technical security of users and company equipment through security awareness/onboarding trainings. SMA Technologies issues documented security policies, updates them as necessary, and provides regular security training for all Staff.

4.2 Background Checks. SMA Technologies ensures that its Staff involved in providing the Services and Support have passed basic background checks designed to validate the completeness and accuracy of resumes, confirmation of professional qualifications, and verification of identity where permitted by law. These checks also include checks of criminal history.

5. Physical and Environmental Security

5.1 Data Transfer. SMA Technologies does not permit Customer Data to be transferred to any external or removable storage media.

6. Communications and Operations Management

6.1 Vulnerability/Patch Management. SMA Technologies has established a vulnerability or patch management process that ensures all systems used to provide the Services and Support, including network devices, servers, and desktops or laptop computers, are patched against known security vulnerabilities in a reasonable period of time based on the criticality of the patch and sensitivity of the Customer Data accessed through the systems.

6.2 Secure System Configuration. SMA Technologies has established controls to ensure that all systems used to provide Services and Support are securely configured in a repeatable manner. This involves changes to default settings to improve system security (*e.g.,* system "hardening"), changes to default account passwords and removal of unnecessary software or services/demons. Additionally, employee devices used to interact or manage systems that provide the Services and Support are to also be configured in a repeatable manner. Specific additional requirements beyond what also exists in this Exhibit include:

6.2.1 Full/whole disk encryption; and

6.2.2 Remote data wipe and lock capability in case of lost or stolen device

6.3 Malware Prevention. SMA Technologies has implemented detection and prevention controls to protect against malicious software and appropriate user awareness procedures. SMA Technologies keeps and updates technical controls and regularly evaluates all systems for the

existence of malware. SMA Technologies runs real-time or regular scans of SMA Technologies' owned devices to detect viruses, malware, and possible security incidents.

6.4 Logging and Auditing. SMA Technologies has in place a comprehensive log management program defining the scope, generation, transmission, storage, analysis, and disposal of logs based on then current industry practices. The systems and the services provide logging capabilities in accordance with the following principles:

6.4.1 the scope of logging and the retention policy is based on a risk-based approach, with minimum retention of six (6) months;

6.4.2 logs are collected to permit forensic analysis on information security incidents;

6.4.3 logs record administrative changes to the Services;

6.4.4 log records are kept virtually secured to prevent tampering;

6.4.5 passwords and other sensitive data elements are not logged under any circumstances;

6.4.6 perform regular log analysis to evaluate security;

6.4.7 configure all affected systems to provide real-time logging of any event that may indicate a system compromise, denial-of-service event, or other security violation, including notifying an administrator when pre-determined event thresholds are exceeded; and

6.4.8 logs are protected from unauthorized access or modification.

6.5 Customer Data Retention. For Customers utilizing only select offerings, SMA Technologies may retain for backup purposes only, limited Customer Data for a minimum of seven (7) days. For more information on data retention, please review our Data Protection Addendum.

7. Disaster Recovery and Business Continuity Planning

7.1 Programs. SMA Technologies has established disaster recovery and business continuity programs and confirms that the plans are capable of ensuring confidentiality and integrity of Customer Data during recovery operations. SMA Technologies also confirms the programs do not allow any reduction of security.

7.2 Backups. It is the Customer's responsibility to back up their database(s) on a regular basis.

8. Security Incidents

8.1 Incident Detection. SMA Technologies has established and maintains an operational incident detection capability and a clearly documented incident response program for responding to suspected or known security incidents or system breaches. Incident response plans include methods to protect evidence of activity from modification or tampering and to properly allow for the establishment of a chain of custody for evidence.

8.2 Incident Response. In the event of an incident that affects Customer Data, SMA Technologies utilizes industry standard efforts to respond to incidents and to mitigate the risk to Customer and Customer Data.

8.3 Incident Notification. In the event of a confirmed incident that affects Customer Data, SMA Technologies will provide notice of the security incident to any relevant Customer within twenty-four (24) business hours of confirmation.

9. Access Control

9.1 Authentication. SMA Technologies supports Single sign on (SSO) mechanisms for Customer to interact with Solution Manager (*e.g.,* Okta).

9.2 Support Access. If SMA Technologies allows its employees to access Customer Data through an application support interface, that interface, at a minimum must uniquely identify the SMA Technologies employee who used it.

9.3 User Passwords. SMA Technologies provides training to its Staff that is reasonably designed to ensure user passwords have sufficient complexity and expiration requirements and where feasible, require an additional layer of security with multi-factor authentication.

9.3.1 Authentication and Two-Factor Authentication. "Two-factor authentication" means the authentication through the combination of something a person knows, such as a username and password, in combination with something a person has, such as a disconnected authentication token, or a biometric factor, such as a fingerprint. SMA Technologies uses multiple authentication factors where available, and SMA Technologies uses at least two-factor authentication to access accounts used to provide data hosting services. All administrative access by SMA Technologies' employees must require two-factor authentication. If SMA Technologies is using Google Apps to manage their accounts, two-factor verification must be enabled.

9.3.2 Inactivity. All SMA Technologies' owned devices automatically lock after a reasonable period of inactivity.

9.3.3 Employee or Consultant Termination. At the time of termination of an employee, contractor, or any third-party consultant, the terminated person's access to the networks, systems, and accounts used to provide the Services and Support, and access to any Customer Data, is terminated.

9.3.4 Authorization. Customer alone controls and provides access to Customer Data.

9.3.5 Network Access Controls. All networks SMA Technologies uses to provide the Services and Support are protected through the use of controls capable of blocking unauthorized network traffic, both inbound (ingress) and outbound (egress).

10. Data Security

10.3 Encryption.

10.3.1 Data in Transit. SMA Technologies ensures that HTTPS is enabled in any web interface related to the product or service. SMA Technologies allows Customer to utilize TLS 1.2 or greater for web-facing applications.

10.3.2 Data at Rest. Customer Data at rest for OpCon on-prem Customers is the responsibility of the Customer. For OpCon Cloud Customers, Customer Data is encrypted at all times using industry-accepted cryptography standards. At a minimum, this includes:

10.3.2.1 Use of Advanced Encryption Standard (AES) defined in FIPS 140-2.

10.3.2.2 Where different algorithms are used, they have comparable strengths (*e.g.,* if an AES-256 key is to be encrypted, an AES-256 key or greater, or RSA-3072 or greater could be used to encrypt it).