Data Protection Addendum

This Data Protection Addendum ("DPA" or "Terms") sets forth the conditions under which SMA Technologies ("SMA") handles your data and is in addition to SMA's Terms and Conditions for the OpCon Solution, Governing Terms for Managed Automation Services. This DPA applies to Customer and all Users who access or use the OpCon Solution in any format.

1. Definitions

The following terms have the indicated definitions and meanings:

"Sensitive Data" means data or information provided by or on behalf of Customer or its affiliates, regardless of form or media, which is:

A. personally identifiable information, including, but not limited to, an individual's: (i) name; (ii) title; (iii) phone number; and (iv) email address;
B. Customer's application or system user ID;
C. data which is specifically identified by Customer as "Sensitive Data;"
D. information Customer may have supplied to SMA for enrollment in SMA's Basic and Advanced Training classes (e.g., emergency contact information).

"SMA" refers to SMA Technologies, and as used in this DPA shall include any contractors, subcontractors, consultants, temporary associates, or other third parties ("Third Party" or Parties") which SMA may utilize to Process Sensitive Data.

"Process or Processing" means any action taken by SMA in relation to Sensitive Data, to include access, collection, use, retention, storage, transfer, disclosure, destruction, and any other operation used for account management, technical support, services as outlined in a separate Statement of Work (SOW), or invoicing purposes.

"Breach" means any confirmed (i) misuse, loss, destruction, compromise, or unauthorized access, collection, retention, storage, or transfer of Sensitive Data or (ii) any act or omission, that causes non-compliance with these Terms.

"Secure Facility" means the physical location(s) where Sensitive Data can be stored or electronically processed. Physical and environmental security controls are implemented to

protect the facility housing system resources, the system resources themselves and the facilities used to support their operation.

All other capitalized terms are defined in SMA Technologies Terms and Conditions and/or Order form.

2. Rights and License in and to Sensitive Data

SMA agrees that as between SMA and Customer, all rights including any intellectual property rights in and to Sensitive Data shall remain the exclusive property of Customer, and SMA has a limited, nonexclusive license to use this data as provided in the Agreement solely for the purpose of performing its obligations thereunder. Neither the Agreement nor this DPA provide SMA any rights, implied or otherwise, to Customer's Sensitive Data.

3. Sensitive Data Handling Requirements

When accessing, storing, processing, or transmitting Customer's sensitive Data or Systems, SMA shall adhere to the following:

A. Prohibition of Unauthorized Use or Disclosure – SMA agrees to hold Sensitive Data in strict confidence. SMA shall not use or disclose Sensitive Data received from or on behalf of Customer except as permitted by the Agreement or this DPA, as required by law, or otherwise authorized in writing by Customer.

B. General Security
   a. process Sensitive Data only in accordance with the terms of the applicable agreement between SMA and Customer, including, without limitation, this DPA;
   b. maintain and utilize a reasonable privacy and security training program applicable to all SMA resources providing services to Customer under the Agreement.
   c. SMA will have in place, written confidentiality agreements or obligations with all of its employees, subcontractors and vendors who work with Customer's Sensitive Data.
   d. protect against any anticipated threats or hazards to the security or integrity of Sensitive Data, including, without limitation:
      (i) reasonable efforts, through the use of industry standard virus and malware protection software and other customary procedures, to avoid introducing or permitting the introduction of any virus into the Customer's IT environment.
      (ii) reasonable efforts to regularly check for and delete viruses and malware in SMA's systems used by SMA to provide the services by way of standard industry virus and malware detection tools.
   e. protect against unauthorized access to or use of Sensitive Data which could result in substantial harm or inconvenience to Customer, including, without limitation:

(i) implementation of administrative, technical and physical security controls to limit access by SMA personnel and Customer authorized subcontractors to only the Customer information they need to provide the services in this Agreement;
(ii) providing user identification and access controls designed to limit access to Customer's systems and information to authorized users, using complex passwords; and
(iii) ensuring that access is revoked for those SMA personnel who no longer have a direct need to have access to Sensitive Data.

f. implement and maintain security policies, procedures, and programs based on industry standards.
g. implement business continuity and disaster recovery plans necessary to ensure systems, services, and information are not unavailable for a period in excess of twenty-four (24) hours.
h. take corrective action(s) to remedy a violation of (and to prevent future violation of) any of these Terms.

C. Security Incidents
   a. contact Customer promptly (in one business day) after a confirmed Breach involving Customer's Sensitive Data.
   b. take prompt corrective action(s) to remedy a Breach and to prevent a future Breach.
   c. take prompt corrective action(s) to remediate any vulnerabilities or security concerns in accordance with SMA's policies.
   d. implement corrective action(s) in a timeframe commensurate with the risk.
   e. cooperate fully with Customer in facilitating investigation and remediation of a Breach.
   f. not inform any third-party of any Breach, except SMA's insurance carrier or as specifically required by applicable law, without first obtaining Customer's prior written consent.
   g. promptly notify Customer's primary SMA business contact of any complaint received related to processing of Sensitive Data.

D. Storing/Transmitting Customer's Sensitive Information
   a. provide evidence of SOC 2 audits for Managed Automation Services and OpCon Cloud Customers.
   b. provide for daily back-up of Customer information and archival of such Customer data for Managed Automation Services and OpCon Cloud Customers. Such is not

applicable to standard OpCon Task-Based Customers who do not subscribe to any type of managed services offered by SMA Technologies.

c. encrypt all SMA storage devices and networks utilizing industry standard encryption techniques.
d. require all SMA personnel to use SMA owned and managed devices to store Customer's information, prohibiting all SMA personnel from using personal computer equipment.
e. prohibit storage to a portable computing device, except Company issued laptops, e.g., USB drives, cameras and camera phones, and any other portable device that would allow the capturing, printing, or storing of Customer's data or confidential information to be transported outside the secure facilities.
f. establish written procedures for the disposal of electronic storage devices and information, which include the destruction and sanitization of all Customer information, compliant with NIST 800-88.
g. if requested, at the conclusion of the Agreement, SMA will certify that all Customer data has been erased from SMA, and all subcontractor and downstream recipient's, equipment; or it has removed the storage device(s) from SMA, and all subcontractor and downstream recipient's, equipment and provided all storage device(s) to Customer, except where SMA has a legal requirement to maintain such data.
h. provide industry standard firewalls, both network and device based, that regulate all data entering SMA's internal data network from any external source, and which will enforce secure connections between internal and external systems and will permit only specific types of data to pass through.
i. prohibit the use of Customer's information in SMA's non-production environments except in instances where information may be replicated on a managed SMA device to reproduce a support issue. In such cases, SMA will have approval to do so from the Customer
    (i) in the form of the Customer's signed Agreement for OpCon Cloud; or
    (ii) by submission of the data by the Customer for OpCon installed on premises.
j. implement audit controls that record and monitor systems activity.

E. SMA Provided Software
    a. not knowingly insert or knowingly allow the insertion into the Software of any code which would have the effect of wrongfully disabling or otherwise wrongfully shutting down all or any portion of the services.
    b. train SMA personnel in proper techniques for developing secure application.

c. upon discovery of software and system vulnerabilities, provide software patches to remediate vulnerabilities.

4. SMA Personnel Requirements

SMA shall ensure that a background check is performed, where allowed by law, on all personnel prior to hiring such personnel if they will have access to Sensitive Data that includes:

A. verification of legal authority to work in the United States and/or other SMA locations, if applicable;
B. review of an individual's record of criminal conviction history. Criminal conviction history checks include a review of all federal, state, and local criminal conviction records.

For purposes of these guidelines, the term "Criminal Conviction" could include any of the following: probation, deferred adjudication, and no contest pleas.

5. Connectivity Requirements

Where SMA is permitted to access any internal Customer systems, applications, or networks (collectively "Customer Systems"), SMA shall:

A. only connect to Customer Systems through the manner and means authorized by Customer.
B. not connect to, access, attempt to access, or use any Customer Systems without the prior authorization of Customer.
C. not use any Customer System in any way that is illegal, abusive or creates a security risk or vulnerability.

6. Off-Shore Processing

Customer data or information must be transmitted or stored electronically using encryption including storage via server storage, backup, copy, paste or similar functions in compliance with applicable local, state, federal or international regulations.

7. Certification and Compliance Requirements

These Terms shall apply to all Sensitive Data which is: (i) Processed by SMA, (ii) provided to SMA by or on behalf of Customer, (iii) learned or otherwise used by SMA during or in connection with the performance of services under the Agreement, or (iv) retained by SMA.

Further, SMA shall provide documentary evidence to Customer to show compliance with the applicable Terms, upon request of Customer. Documentary evidence may include summaries of SMA's applicable security policies and standards, and/or written certifications of Sensitive Data destruction.

8. Third-party Compliance

SMA shall be solely responsible and liable for ensuring that any third-party subcontractor who Processes Customer's sensitive Data as part of SMA's performance under the Agreement fully comply with this DPA.

9. Non-Compliance

SMA's failure to comply with any Term shall be a breach of the Agreement(s) with Customer. Without limiting any other right or remedy that Customer may have, Customer has the right to terminate, for default or breach, the Agreement as a result of such noncompliance in accordance with the terms of the Agreement.

10. Vulnerability Tests

In the event that any Customer's sensitive Data is processed or available through SMA's website, SMA shall conduct, at the very least, annual vulnerability tests.

11. Survival of Requirements

These Terms shall remain in effect so long as SMA has any Customer Sensitive Data, regardless of any termination, amendment, or executions of other agreements, and shall remain in effect until SMA has destroyed or returned all Sensitive Data to Customer. Where retention of Sensitive Data is required by law, these Terms shall remain in effect for the period required by applicable law, after which time, SMA shall destroy or return all Sensitive Data, in accordance with these Terms.

12. Indemnity

SMA shall defend and hold Customer harmless from all claims, liabilities, damages, or judgements involving a third-party, including costs and attorney fees, which arise as a result of SMA's failure to meet any of its obligations under this Agreement.

Effective Date: October 10, 2022