Information Security Exhibit

General Security Measures:

Uniphore will comply with industry standard security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, and incident response measures necessary to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer's information provided by Customer to Uniphore), as well as with all applicable security laws, regulations and standards.

1. Definitions:

   a. Authentication means the process by which a person, process or system is verified as a particular person, process or system or a member of a class of persons, processes, or systems, typically for access to data or another right or privilege.

   b. Confidential Information means non-public information received from Customer as defined in the Agreement.

   c. Personal Information means any information that relates to or describes an individual or household, including any data that is linked or linkable to an individual or household.

   d. "Security Incident(s)" shall have the meaning assigned by Applicable Data Protection Law(s) to the terms "security incident," "security breach" or "personal data breach.

2. Information Security Program:

   Uniphore maintains an information security program ("Information Security Program") designed to implement technical and organizational measures to protect Customer data as required by Applicable Law(s), the Agreement, and this Exhibit. Uniphore agrees to implement and train its employees on its Information Security Program.

   a. Access control. Access to systems containing stored Customer data will not be granted to Uniphore' employees, subcontractors, or other agents unless: (i) they have a need to view the information in order to perform authorized work; (ii) they are trained in the proper handling of Customer Confidential Information; (iii) they are subject to an obligation to handle Customer data in ways at least as restrictive as those practices outlined in this Exhibit; (iv) their access can be uniquely identified (e.g., by a unique User ID), (v) they are required to use a password or other authorizing token configured to meet industry best practice standards, (vi) they are permitted access only as required to perform their job function, (vii) the date, time, requestor, and nature of the access (i.e. read-only or modify) is recorded in a log file which is maintained and preserved according to Applicable Law(s) and industry standards and (viii) access is only granted on least privilege/need-to-know basis.

- Compliance. Uniphore complies with ISO 27001:2013.

b. Storage. Uniphore agrees to (i) store Customer data with access to such data limited as described in 2(a).

c. Procedures for Changing Roles. Uniphore has procedures in place to modify or revoke access permissions to Customer data when job responsibilities change and/or need for data access changes.

d. Encryption. Uniphore agrees to (i) adopt commercially reasonable industry practices with regard to encrypting Customer data and (ii) transmit data over secure and encrypted connections using industry-standard encryption techniques.

e. Human Resources Security. Uniphore shall maintain a policy which defines requirements around enforcing security measures as they relate to employment status changes. This includes background checks, acknowledgement, and adherence to Uniphore's security policies, onboarding, and termination for employees and third parties.

f. Physical and Environmental Security. Uniphore maintains policies and procedures for physical and environmental security, define requirements to protect areas that contain sensitive information and ensure that critical information services be protected from interception, interference, or damage.

g. Third-Party Risk Assessments. Uniphore conducts security due diligence on its third-party service providers, including subcontractors, to assess and monitor risk. This assessment includes a review of scope of confidential information and/or personal data transferred to or processed by the service provider and the purpose of the work. Uniphore also conducts risk assessments on its third-party service providers which may include auditing the service provider's organization and technical security measures and assessing the sensitivity of any information processed by the service provider, storage limitations, and data deletion procedures and timelines.

h. Printed Material. With respect to printed material containing Customer Confidential Information, Uniphore agrees (i) to store such material in secured areas with access limited to individuals with business need to access, and (ii) that such material will be disposed of in a secure manner employing processes including onsite shredding prior to recycling or placement in secure bins.

i. Network Scans. Uniphore runs internal and external network vulnerability scans periodically and after any change in the network configuration (such as new system component installations, changes in network topology, firewall rule modifications, or major product upgrades).

j. Vulnerability Remediations. Uniphore regularly deploys application security testing and vulnerability scans as part of its software development lifecycle process. Detected vulnerabilities are evaluated according to the NIST Common Vulnerability Scoring System (CVSS) to determine the severity. Where a vulnerability is detected in 3rd party software that is incorporated in Uniphore software, Uniphore may depend on remediation and fixes from the 3rd party vendor before a patch or service pack can be issued for Uniphore software. If a software patch is required, Critical vulnerabilities will be patched as soon as reasonably possible, High vulnerabilities are targeted for the next planned service pack if reasonably possible. Medium and Low severity vulnerabilities are tracked and incorporated into standard release planning and development cycles for regularly scheduled releases.

k. Security Fixes. Uniphore agrees to promptly install any security-related fixes related to Customer Confidential Information.

l. Security Threats and Associated Modifications. Customer may, from time to time, advise Uniphore of recent security threats that have come to its attention and recommend Uniphore to implement specific modifications of their software, policies, or procedures. To the extent such modifications are needed to comply with Uniphore's obligations under Applicable Law(s), the Agreement, this Exhibit, or any applicable Order Form, Uniphore agrees to (i) implement the recommended modifications or (ii) implement alternative modifications guaranteeing a level of protection equal to or superior to the level of protection granted by the modifications recommended by Customer.

m. Testing Key Controls, Systems and Procedures. Notwithstanding the minimum standards set forth in this Exhibit, Uniphore agrees to regularly test the key controls, systems, and procedures of their Information Security Programs to ensure that they are properly implemented and effective in addressing the threats and risks identified, and incorporate reasonable, industry-standard, security safeguards. Tests will be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the Information Security Program as needed.

n. Hardware and Electronic Media. Uniphore will deploy and follow policies and procedures to ensure (i) the safe receipt and removal of hardware and electronic media containing Customer data into and out of a Uniphore' facilities as applicable, (ii) the movement and storage of these items within Uniphore' facilities, (iii) the disposition of the hardware or electronic media on which it is stored, and (iv) the removal of Customer data from electronic media before re-use.

o. Storage Media. Uniphore will deploy and follow policies and procedures to ensure that all Customer data is irreversibly and securely deleted from storage media prior to any such storage media (i) being assigned, allocated or reallocated to another individual, or (ii) being permanently removed from Uniphore' facilities. Uniphore agrees to maintain an auditable program implementing the disposal and destruction requirements set forth under Applicable Law(s) and this Exhibit for all storage media containing Customer Confidential Information.

p. Authentication. Uniphore will protect all Confidential Information prior to granting access to Confidential Information stored in a system, application, or database. Authentication resulting in access to a system, application or database containing Confidential Information will be logged consistent with these Requirements. Uniphore will implement multi-factor authentication for Uniphore personnel for all remote access to Confidential Information hosted by Uniphore.

q. Cloud Environments. For all Cloud Environments, Uniphore will validate compliance, at least once annually, with a set of security and privacy controls which will meet the compliance requirements set out hereunder for the protection of Confidential Information.

Secure Software Development Uniphore will maintain policies and procedures to ensure that system, device, application, and infrastructure development is performed in a secure manner. This includes review and test of all Uniphore applications, products and services for common security vulnerabilities and defects, employing defense-in-depth strategy using multiple layers of security boundaries and technologies, periodic penetration testing and security assessment of these services, defining baseline

configurations and requirements for patching of third-party systems.

r. Assessments, Audits and Remediation

a. Assessments. Records to demonstrate compliance with this Exhibit and Applicable Law(s) will be maintained by Uniphore and provided to Customer upon request.

b. Audits. To verify Uniphore' compliance with Applicable Law(s) and this Exhibit, Uniphore agrees to provide independent third-party audit reports to Customer upon written request by Customer.

c. Remediation. Uniphore agrees to (i) promptly take reasonable action to correct any material security issue affecting Customer Confidential Information, and (ii) forthwith promptly inform Customer upon discovery of such actions if it is related to a Security Incident affecting Customer Confidential Information.

s. Secure Disposal. Customer data shall be securely disposed (i) during the duration of the Agreement upon Customer's written request if such information is no longer reasonably required to perform the Services, (ii) within ninety (90) days of the termination of the provision of the Services, subject to requirements of Applicable Laws. Uniphore may retain Customer data to the extent that it is required to do so under Applicable law(s). When disposing of Customer Confidential Information, Uniphore agrees to destroy and/or delete such data from any media (including back-up copies) such that the media contains no residual data and to certify in writing to such destruction and/or deletion upon request.

t. Security Incident

a. Security Incident Procedure. Uniphore agrees to deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents pertaining to Customer data including procedures to (i) monitor systems and detect successful and attempted attacks on or intrusions into or information systems relating thereto, (ii) identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, in each case, as they pertain to Customer Confidential Information, and (iii) restore the availability or access to Customer data in a timely manner. Customer agrees to notify Uniphore of any known or suspected Security Incident. The obligations described in this Section shall not apply in the event that a Security Incident results from the actions or omissions of Customer. Uniphore's obligation to report or respond to a Security Incident will not be construed as an acknowledgement by Uniphore of any fault or liability with respect to the Security Incident.

u. Notice. Uniphore agrees to provide prompt written notice as soon as reasonably practicable but in no event later than forty-eight (48) hours of discovery, if it knows that a Security Incident pertaining to Customer data has taken place.

v. Contact Information

a. Uniphore agrees to designate a point of contact as Security Coordinator. This Security Coordinator will:

(i) maintain responsibility for applying the relevant protections to Customer Confidential Information, including the development, implementation, and maintenance of its Information Security Program,

b. (ii) oversee application of Uniphore' compliance with the requirements of this Exhibit, and (iii) serve as a point of contact for internal communications and communications with Customer pertaining to this Exhibit and compliance therewith or any breaches thereof.

c. Additionally, both Customer and the Uniphore agree to designate a point of contact for urgent security issues (a "Security POC") and provide contact information for such Security POC. The Security POC for both parties are:

Customer Security POC:
Uniphore Security POC: infosec@Uniphore.com