EXHIBIT __
INFORMATION SECURITY

This Exhibit sets forth certain duties and obligations of [Supplier] with respect to the protection, security and privacy of information disclosed in the course of performance under the Agreement. This Exhibit is incorporated into and subject to the terms and conditions of the Agreement. In the event of inconsistencies between this Exhibit and the Agreement, the Exhibit shall supersede and control.

1.0 DEFINITIONS:

1.1. **"Company Data"** means all Confidential Information and Personal Data whether provided pursuant to a Statement of Work (or other contractual agreements), project specifications, documentation, software or equipment by or on behalf of Company, its Affiliates, and/or its customers and information derived from such information, including as stored in or processed through diagnostic tools, hardware, firmware or software.

1.2. **"Company Personnel"** means Company employees, officers, directors, agents, contract workers and subcontractors, applicants for employment at Company and applicants seeking to work as a Company contract worker or subcontractor and also includes all such persons when associated with Company Affiliates.

1.3. "**Cybersecurity Measures**" means the mechanisms or controls used to protect or defend the use of cyberspace from cyber-attacks.

1.4. **"GDPR"** means the General Data Protection Regulation (EU) 2016/679 ("EU GDPR"), the United Kingdom General Data Protection Regulation, as it forms part of UK law by virtue of section 3 of the EU (Withdrawal) Act 2018, and the UK Data Protection Act 2018, ("UK GDPR"), and the revised Swiss Federal Act Data on Protection Act ("FADP").

1.5. **"Information Processing System(s)"** means the individual and collective electronic, mechanical, or software components of Supplier operations that store and/or process Company Data.

1.6. **"Malicious Code"** means any computer instructions that are not intended to provide the functionality described and that interfere with or prevent Company use as contemplated in this Agreement. Malicious Code includes, without limitation, computer viruses and any other computer instructions that interfere with or prevent Company from using the Company systems, Company Information or as described in its specifications or as contemplated in this Agreement. Malicious Code also includes, without limitation, any computer instructions that can: (i) disable, destroy, or otherwise alter the Company Information or any hardware on which it executes; or (ii) reveal any data or other information accessed through or processed or stored by the to anyone outside of Company without Company' knowledge and prior approval.

1.7. **"Personal Data"** means information that can be used to identify, locate, or contact an individual, alone or when combined with other personal or identifying information to the extent that such information is protected as personal data, Personal Data, personally identifiable information (or a similar term) under the Privacy Laws.

1.8. **"Privacy Laws"** means all applicable U.S. and international laws that regulate the Processing of Personal Data, which may include but are not limited to GDPR and the California Consumer Privacy Act.

1.9. "**Process**", "**Processing**" or **"Processed**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.10. **"Provider"** means any third-party with access to Company Data by, through or under Supplier including sub-contractors of whatever tier.

1.11. "**Ransomware**" is a type of malware threat actors use to infect computers and encrypt computer files and/or data until a ransom is paid. After the initial infection, ransomware may attempt to spread to connected systems, including shared storage drives and other accessible computers.

1.12. **"Security Incident"** is an event that may potentially disclose Company information or make information unavailable. Security Incidents will be considered confidential and will be treated in accordance with the confidentiality requirements of this Agreement, except notice to Company Personnel, company's customer, or other parties pursuant to Privacy Laws or Company policy.

1.13. **"Vulnerability"** is a weakness or flaw in a system, network, application, or device that can be exploited by a threat actor to gain unauthorized access, disrupt operations, or compromise data integrity and confidentiality.

2.0 SECURITY REQUIREMENTS:

2.1. Supplier represents and warrants that it implements and maintains and will implement and maintain for the duration of this Agreement security measures in accordance with industry standards (such as the Payment Card Industry Data Security Standard or PCI DSS), and applicable law, for electronic and other media that are suitable to protect the security of information processed or stored, including, without limitation:

2.1.1. Industry-standard administrative, technical, and physical measures to protect against and detect unauthorized destruction, loss, alteration, use, disclosure, access, misappropriation, or ransoming of Company Data (collectively, "Cybersecurity Measures").

2.1.2. Implementation of detection, prevention, and recovery controls to protect against Malicious Code, including training its personnel on such protections.

2.1.3. Reliable, industry-standard cybersecurity and spam filtering software(s), including industry-standard Advanced Threat Protection.

2.1.4. Monitoring of Supplier's computer and network systems and data for unauthorized destruction, loss, alteration, use, disclosure, access, misappropriation or ransoming by unauthorized persons (a "Breach").

2.1.5. Requiring its Providers to securely and safely dispose of media (including but not limited to hard copies, disks, CDs, DVDs, optical disks, USB devices, hard drives)

containing Company Data when no longer required by the establishment of procedures.

2.1.6. Holding its Providers to similar security standards as outlined in this agreement, including, but not limited to, Security Incident notification of incidents which may or have impacted Company.

2.1.7. Encrypting using best industry practices all Company Data in transit and at rest, including offline back-up copies thereof, stored by Supplier at Supplier's data center that are tested at least annually.

2.2. Supplier will identify in writing and make available, upon request, to Company the system security standards and documented processes used to secure Supplier's systems. Supplier and/or Supplier's third-party processors will provide certifications that it meets the minimum standards of (a) NIST Cyber Security Framework (b) International Standard ISO/IEC 27001:2013 or its successors, (c) SOC 1 Type II or/and SOC 2 Type II, (d) International Standard ISO/IEC 27018:2019 or its successors. If Supplier is not ISO or SOC certified or has other information based on region of location, Supplier shall provide documentation on industry best practices being followed.

2.3. As defined in 2.2, upon request and with 30 days' notice unless due to a Security Incident, Supplier and/or Supplier's third-party processor(s) will provide an audit report for review by Company. If Supplier is not compliance certified, Supplier shall provide internal audit results.

2.4. Supplier will have a Security Incident response process in place to manage and to take immediate corrective action for any Security Incident.

2.4.1. In conjunction with Section 3.0, Supplier shall have plans specific to Ransomware, including playbooks on how these situations should be dealt with.

2.5. Supplier will secure all areas, including loading docks, holding areas, telecommunications areas, cabling areas and off-site areas that contain Information Processing Systems or media containing Company Data, by the use of appropriate security controls in order to ensure that only authorized personnel are allowed access and to prevent damage and interference.

2.6. Supplier shall implement:

2.6.1. (a) user authentication and access controls for all operating systems, networks, and related equipment, including protocols governing secure remote access and (b) prohibition against use of employee-owned personal computers, smart phones, and other technological equipment directly accessing Supplier's network, except for email access.

2.6.2. Measures to ensure that all systems and software are kept up-to-date and fully functional, with minimum standards for functionality and update frequency.

2.6.3. Backup of all Company-related data on a daily basis in multiple locations and/or via multiple medias (including the use of offline backup and immutable storage, to the maximum extent possible).

2.7. Supplier will not store Company Data on personally owned equipment and/or services not controlled by Supplier.

2.8. Supplier will ensure that access to source code is restricted to authorized users who have a direct need to know.

2.9. Supplier will develop configuration standards for all system components that address all known Security Vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Institute (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

3.0 SECURITY INCIDENTS:

Supplier shall notify Company of a Security Incident as soon as practicable, but no later than seventy-two (72) hours after Supplier (including Providers) becomes aware of a Security Incident by sending notice to cyberir@clarios.com. Notification will include the occurrence of any unauthorized access, use, violation, compromise, or breach of security (electronic or physical), involving Company Data or the computing environment, information or communication systems, facilities, equipment, or transportation means involved in handling of Company Data. Supplier will cooperate, work with, and provide necessary information concerning such breach to allow Company to evaluate the likely consequences and any legal or regulatory requirements arising out of the event unless the sharing of such data is prohibited by law. Supplier shall use its best efforts to immediately terminate any security breaches or suspicious activity. Supplier shall not allow any security breach or suspicious activity to persist for any amount of time or for any reason except as required by law, or as deemed reasonably necessary by Supplier to stop such breach or suspicious activity. If any breach of the integrity, confidentiality, availability, or privacy of the Company Data requires notification by Supplier to any party under any of the Privacy Laws, Company and Supplier shall collaborate to define the timing, content, and method of such notification. Supplier shall reimburse Company for its out-of-pocket costs in providing the notification.

3.1 Subsequent Reports and Notifications: After the initial notification, Supplier shall subsequently update Company's security team on Supplier's efforts with respect to Security Incidents via the email address noted above and/or a dedicated teleconference bridge-line established for the event. Such notifications shall occur on a negotiated regular basis.

3.2 Security Incident Resolution: Supplier shall provide Company with written documentation of the cause, remedial steps and future plans to prevent a recurrence of the same or similar breach or suspicious activity. Supplier shall immediately implement the proposed remedial plan or discuss for a mutually agreed upon timeframe. If such remedial plan is unacceptable, based on Company's reasonable judgment, Supplier shall promptly but in any event no later than five (5) days enter into good faith negotiations to address the proposed remedial plan. Supplier shall reasonably cooperate with Company security investigation activities and with the preparation and transmittal of any notice or any action, which Company in its sole discretion may deem appropriate or required by law, to be sent or done for customers or other affected third parties regarding any known or suspected security breach.

3.3 Final Report: Supplier shall provide Company, with a final written report of each Security Incident within three (3) business days of resolution or a determination that the problem cannot be satisfactorily resolved within such time period (in which case, an estimated date for final resolution shall be proposed). The report, to the extent that is possible may include:

- Supplier's Name.
- Supplier's Incident Coordinator and contact information.
- Date Incident Occurred and Length of Outage.
- Incident Executive Overview.
- Incident Details:
    - How/when the incident was initially detected.
    - When/How the incident was initially reported to Company.
    - Description of what resources/services were impacted.
    - Description of impact of Security Incident to Company (volume and type where applicable).
    - Containment – How was the incident contained.
    - Root Cause - What was the cause for disruption.
    - Corrective Action During the Incident – What steps were taken to reduce exposure during the incident (in most cases, there are interim steps taken to reduce exposure, e.g., Filtering, rerouting services, etc.).
    - Permanent Corrective Action/Preventative measures – What permanent corrective actions have been put in place as a result of this incident.
- Conclusion.

3.4 Right to Security Assessment: In the event of a Security Incident, Company shall have the right to conduct or contract with a third party to conduct an Assessment, to validate that all necessary and timely remedial actions have been taken by Supplier to correct the Security Incident. In addition to the foregoing, Company shall have all rights and remedies available to it as outlined in the Agreement and/or as otherwise prescribed by United States law.

3.5 Supplier shall maintain logs of all Security Incidents and will support Company in our investigation of a possible Security Incident via MS Teams or other mutually agreed upon application upon request. Logs shall minimally be a summary, including date and information on incident (not including other client details if applicable).

4.0 SUPPLIER'S INTERNAL AND PROVIDER USER ACCESS SECURITY:

4.1 Subject to local law and jurisdiction, background checks must be performed and documented prior to permitting Supplier personnel to have access to Company Data. Company reserves the right to ask for proof that background checks are occurring, Company will not request actual background checks nor confidential data, rather evidence the process was performed.

4.2 Supplier must employ a formal user registration and de-registration procedure for granting and revoking access and access rights to all Information Processing Systems.

4.3 If Company agrees that any portion of the [Work] may be subcontracted; All sections of this exhibit shall apply equally to the Subcontractor.

5.0 OWNERSHIP AND TREATMENT OF COMPANY AND PERSONAL DATA:

5.1 Access to any Company Data: (a) shall be subject to compliance with all applicable Company policies and procedures, (b) shall be limited solely to such Company Data as is required for Supplier to perform its obligations under the Agreement, and (c) may be restricted or revoked by Company in its sole discretion at any time without notice. Supplier will not grant access to Company Data to any third party or use any third-party computer systems to access Company Data without first obtaining Company's written consent.

5.2 Company Data will be and remain, as between the parties, the property of Company. Supplier will not modify, reformat, reorganize, store, transfer, or delete Company Data in any manner except as permitted by the Agreement or without the express written consent of Company and only in the manner permitted in writing by Company. Supplier will not possess or assert any lien or other rights against or to Company Data. No Company Data, or any part thereof, will be commercially exploited by or on behalf of Supplier. Company shall own and retain all right, title and interest, including all intellectual property rights, in and to all Company Data and any information submitted to the applications by its users that is not otherwise Supplier's confidential information. Supplier acknowledges and agrees that notwithstanding any reformatting, modification, reorganization or adaptation of the Company Data (in whole or in part) during its incorporation, storage or processing, or the creation of derivative works from the Company Data, the Company Data will remain as such and will be subject to the terms and conditions of this Agreement. This Agreement does not grant to Supplier any license or other rights, express or implied, in the Company Data, except as expressly set forth in this Agreement.

5.3 Encryption of Company Data – Transmission. When Processing Company Data, connections to Company computing environments and any other transmission via data transmission services or using the Internet will be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP, or other technologies that provide substantially similar or greater levels of security. Encryption algorithms will be of sufficient strength to protect data to commercially reasonable security levels and will utilize industry recognized hashing functions. Transmission may not use any cryptography algorithms developed internally by or for Supplier. Encryption must be in full compliance with export laws applicable to the Company Data being transmitted.

5.4 Encryption of Company Data – Storage. Storage, back-up or other retention of Company Data at rest will be protected using one or more of the encryption technologies approved in this Exhibit for data transmission.

5.5 Back-up, Emergency/Disaster Recovery Systems. Applying the requirements of this Section to Company Data stored on back-up media, servers or repositories, transported, or transmitted, stored or recovered as part emergency or disaster recovery systems maintained by or for Supplier.

5.6 Information Retention and Disposal. (i) Cooperating with Company in administering its retention requirements concerning Company Data and employing Record controls

required to enable such compliance, and (ii) returning or if authorized by Company, discarding, destroying and otherwise disposing of Personal Data in a secure manner to prevent unauthorized Processing of Personal Data consistent with Company policies and applicable law.

6.0 COMPANY NETWORKS:

6.1 If access to any Company computer network ("Company Network") is required by Supplier, then Company shall determine the nature and extent of such access. If remote access is given to Supplier, then information relating to such remote access shall be considered Company's Confidential Information. In addition, access to a Company Network shall be subject to the following:

6.1.1. Company's Network will be used by Supplier solely to perform its obligations under the Agreement.

6.1.2. Access to a Company Network will be restricted to Supplier's Personnel who need access for Supplier to fulfill its obligations under the Agreement; and no access rights will be transferred to any other individuals without the prior written consent of Company.

6.2 Without limiting any of its other rights, Company shall have the right to restrict and monitor the use of the Company Network, and to access, seize, copy and disclose any information, data or files developed, processed, transmitted, displayed, reproduced or otherwise accessed on a Company Network. Company may exercise its rights reserved hereunder: (a) to ensure compliance by Supplier's Personnel with Company's policies and procedures while on a Company Network; (b) to work with Supplier to investigate conduct that may be illegal or may adversely affect Company; and (c) to prevent inappropriate or excessive personal use of any Company Network. Supplier will advise its Personnel concerning the rights stated hereunder.

6.3 While on Company's premises, Supplier will not connect hardware (physically or via a wireless connection) to any Company Networks unless necessary for Supplier to perform services under this Agreement or a SOW and only with Company's prior consent. Company has the right to inspect or scan such hardware before or during use.

6.4 Business to Business Connections - Access to and from Company's Network to internal, external, Provider and public network services that allow access to Information Processing Systems shall be controlled. Such connections will:

6.4.1. Ensure that current industry best practice standard authentication mechanisms for network users and equipment are in place and updated as necessary.

6.4.2. Ensure electronic perimeter controls are in place to protect Information Processing Systems from unauthorized access.

6.4.3. Connections will terminate in the Company's DMZ.

6.4.4. Ensure authentication methods are used to control access by remote users.

6.4.5. Ensure physical and logical access to diagnostic and configuration ports are controlled.

7.0 SUPPLIER'S PATCHING, VULNERABILITY AND PENETRATION TESTING:

7.1 As applicable to the services provided under the Agreement, at least once per year (or more frequently if requested by Company or required by applicable law or industry standard), Supplier shall conduct or arrange for vulnerability assessment and penetration testing of Supplier's security processes and procedures, including vulnerability assessment and penetration testing of its services and deliverables under the Agreement, in order to identify potential Security Vulnerabilities. Supplier shall conduct, arrange, or validate testing on all computers and systems used directly or indirectly in support of Company business.

7.2 Supplier shall select an independent, qualified vendor to conduct the testing, sending upon request an executive summary of the testing results including any vulnerabilities corrected (Without disclosing any security privacy protections).

7.3 Supplier shall regularly patch and update software and OSs to the latest versions, ensuring devices are properly configured and that security features are enabled.