Information Security Requirements

This Information Security Requirements Exhibit ("Exhibit") is an attachment to and incorporated into the Agreement. In the event of a conflict between this Exhibit and any other terms of the Agreement (including but not limited to any attachment, statement of work, order, exhibit, referenced URL, etc.), the language that is more protective of Company and Company Confidential Information shall govern. Capitalized terms used but not defined herein will have the meanings set forth in the Agreement.

1. General Terms. Below are frequently used definitions and terminology in this Exhibit:

   a. "Personal Information" – Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household. Personal Information obtained by Vendor independent of the Agreement is not considered Personal Information for the purposes of this Exhibit unless it is used for or in connection with the Services in some capacity.

   b. "Restricted Information" – Any Company Confidential Information that (i) is labeled "Restricted" or "Private;" (ii) is or includes Personal Information; or (iii) if the contents of the data are reasonably known to the Vendor, is of the type or nature where its loss or alteration could reasonably be expected to have a significant impact on Company’s or its Affiliates’ clients or business.

   c. "Confidential Information" – Will have the meaning set forth in the Agreement, but for purposes of this Exhibit will include all non-public information shared between the Parties and/or used in the performance of Services. Confidential Information includes all Personal and Restricted Information.

   d. "Subcontractor" – Any third party involved in the performance of Services or who otherwise has access to Company Confidential Information or Systems.

2. Baseline Security Requirement. Vendor will use and maintain organizational, administrative, and technical controls that meet or exceed applicable and currently accepted industry standards to protect Company Confidential Information from unauthorized access, impact to availability, and alteration/destruction. Such controls must always comply with Law. Vendor will use reasonable efforts to keep Confidential Information isolated and separate from data of other third parties.

3. Subcontractors. In addition to Vendor’s obligations set forth in the Agreement, Vendor will cause all Subcontractors who process or access Company Confidential Information to enter into a written agreement that commits the Subcontractor to adhere to security requirements no less rigorous than those set forth in this Exhibit.

   a. Vendor must obtain additional written consent (notation within a SOW sufficient) prior to permitting a Subcontractor to process or access Company Personal Information. Vendor will maintain list of all such Subcontractors and furnish it to Company upon request.

4. Incident Response. Vendor will adhere to the incident response obligations set forth in the Agreement.

5. On Site Personnel; System Access. If any Vendor Personnel accesses Company's facilities, network, or information technology assets ("Systems") during the performance of Services, such Vendor Personnel must comply with Company’s information security and physical security policies and procedures when doing so. Company may remove Vendor Personnel from its facilities or rescind access to its network or information technology assets at its sole discretion. Vendor will maintain a list of all Vendor Personnel and Subcontractor Personnel who have access to Systems and furnish that list to Company upon request. Vendor will notify Company as soon as possible, but never in more than eight (8) hours, should Vendor Personnel or Subcontractor Personnel no longer require access to Systems or if they are no longer employed by Vendor or Subcontractor.

6. Encryption. Vendor will not perform Services using, nor store any Company Confidential Information on, any portable device or media (including laptops, USB storage devices,
smartphones, etc.) that does not use at least industry standard, full disk (where possible) encryption.

a. Vendor will encrypt all Personal Information and other Restricted Information in transit and at rest using an encryption standard/algorithm with no compromises (for example, Advanced Encryption Standard (AES)) and with a key length of 256-bit or higher. In doing so, Vendor will use reasonable encryption key management techniques to protect against compromise of keys and, consistent with Section 3 of this Exhibit, will notify Company of any suspected or actual compromise of an encryption key used to decrypt any Company Confidential Information.

7. Information Security Audit. At Company’s request, and no more than once per year, Vendor grants Company all necessary permissions and access rights to those Vendor facilities and systems used in the performance of Services to perform an audit of Vendor’s adherence to this Exhibit as further detailed below (“Security Audit”). Vendor agrees that Company (or at its election, an agent or an independent third party agreed to by the Parties) may conduct additional Security Audit(s) during the same year if (i) the initial audit identifies a material audit finding (in which case Company is entitled to audit the non-compliant control(s) until such material finding is remediated), (ii) Company witnesses or has reasonable grounds to suspect non-compliance with this Exhibit, or (iii) Company receives notification of a Security Incident pursuant to the Agreement. Vendor will cooperate with the Security Audit by providing access to: relevant policies, procedures, and documentation; knowledgeable personnel; in scope systems and networks; any additional information at the reasonable request of Company, and where possible, those same elements for any Vendor Subcontractor used directly or indirectly in the provision of Services. To the extent Vendor provides Services that use internet facing sites and/or applications, the Parties agree that Company may request Vendor to provide an executive summary of any third-party vulnerability scan reports related to such site(s) as part of the Security Audit. Should Vendor not have such a report, Vendor agrees, at its exclusive cost, to engage a mutually agreed to third party to perform vulnerability testing on the in-scope sites and/or applications. For environments where Company is not Vendor’s exclusive tenant, Vendor will take all reasonable steps to provide the above access, however in doing so, will not need to disclose information or provide access to particular systems (or environments within the system) that would violate Vendor’s confidentiality obligations to co-tenants. At its exclusive cost, Vendor will promptly remediate any audit findings, and to the extent Vendor disagrees with such finding, work in good faith to negotiate a mutually satisfactory mitigation strategy. To the extent that Company and Vendor cannot reach agreement on a mitigation strategy for a material audit finding, Company will have the right to terminate the Agreement for convenience, in whole or in part, but in no event with greater than thirty (30) days prior written notice without penalty, liability, further obligation, or prejudice to other remedies Company may have. Upon agreement between the Parties, Company may elect in writing to accept an independent verification (e.g. FedRamp, CSA Certification for cloud deployments, HiTrust, SOC 2 Type II, etc.) in place of a full Security Audit. Vendor grants Company the above security audit rights throughout the term of the Agreement and for as long as Vendor retains any Company Confidential Information.

8. Access Controls. Vendor will restrict access to Company Systems and Company Confidential Information on a need basis using the principle of least privilege. Unless otherwise specifically approved in an SOW, Vendor will maintain the Company operating environment (including any Company Confidential Information) in a segregated state from Vendor internal environments or those environments used by/for other clients such that only authorized Vendor Personnel or Subcontractors providing Services to Company may gain access.

a. Vendor will use at least reasonable authentication controls that include to: (i) complex password requirements of seven or more characters with at least three of: case sensitive, letters, numbers, and special characters; (ii) periodic forced password changes no less than every sixty (60) calendar days; (iii) account lockout after no more than eight failed attempts; (iii) prohibit group or shared accounts / passwords; (iv) prohibit use of default passwords; and (v) minimum password age of one day.
b. Vendor must use two-factor authentication for (i) all accounts with privileged or elevated access rights to Systems or applications hosting or processing Company Confidential Information, and (ii) any remote access by Vendor to Systems or Company Confidential Information.

c. Vendor must perform access reviews at a minimum twice annually to confirm appropriate access related to services provided. Vendor will perform timely de-provisioning of access at time of termination.

d. Vendor must perform logging and monitoring of access related activities.

9. Viruses and Malware. Vendor will deploy and maintain (using automated virus signature updates) reasonable anti-virus / malware software on all servers and workstations involved in providing the Services or that access Company Confidential Information as well as where necessary to scan all Vendor inbound network traffic. Additionally, Vendor will configure the anti-virus software to perform periodic endpoint scans and promptly remediate any findings.

a. In cases where Vendor will deliver a Work Product, and to the extent applicable, the Services, will not contain any security defect, including any malware, vulnerability, virus or any mechanism, including any worm, lock, drop-dead device, Trojan horse routine, trap door, time bomb, or any similar code or instruction that will:

i. Delete, disable, interfere with, or otherwise harm the software (or Company hardware, data, or other programs or products).

ii. Make the Services, Work Product, or Confidential Information or Systems inaccessible to Company.

iii. Permit any third party to access Confidential Information or Systems or take any of the actions described in aforementioned subsections above.

10. Web-Enabled Applications. All internet facing sites used in connection with the Services and that either host Company Confidential Information or are accessed by Company Personnel or Company clients must use industry standard tuned and configured Web Application Firewall (WAF) and must be scanned and remediated using accepted industry standard tools for security vulnerabilities (e.g. Open Web Application Security Project and Open Web Application Security Project Top 10). Scan and remediation must first be completed prior to the implementation of the applicable Service. Post-implementation, Vendor will conduct scans at a frequency that is appropriate for the relevant application, technology, and data risk. Websites will implement and maintain accepted industry standard account and password management controls, including:

a. Lockout after no more than 8 unsuccessful login attempts;

b. Prohibiting user IDs, passwords and personal data from being displayed in a URL;

c. Storing user passwords and reset/forgotten security questions in an encrypted manner;

d. Re-authentication is required after no more than 15 minutes of inactivity; and

e. Prohibiting the storage of passwords or personal data in persistent local storage (caches, etc.) or in any cookies, Javascript, or other web tracking technology.

11. Software Coding and Application Development Security. Vendor will implement appropriate technical and organization measures to ensure the delivery of secure code (for example, the OWASP Application Security Verification Standard (“OWASP Verification Standard”)), including but not limited to strong configuration management, application security testing, runtime exploit prevention and no vulnerable open source code. Vendor’s development will not be complete until the security of the code and application has been demonstrated via a security report. Such security report must be provided by Vendor and reviewed and accepted by Company.

12. Awareness and Training. Vendor will provide information security awareness training to all its Personnel with access to Company Confidential Information or Systems that materially cover the security requirements of this Exhibit.

13. Test Environments. Without Company’s prior written consent, Vendor may not store, transmit, access or display Personal Information or any production data within any non-production
computer systems environment including to computer system environments designated as development, quality assurance or test.

14. **Physical Security Requirements.** All security requirements, controls, and standards contained within this Exhibit apply equally to physical / tangible assets (including any Confidential Information in paper format) and facilities wherever feasible.

15. **PCI.** To the extent Vendor stores, transmits, or processes cardholder data (as defined by the Payment Card Industry Data Security Standard, "PCI-DSS") Vendor will comply with PCI-DSS, as well as obtain and maintain third party PCI-DSS certification. Vendor acknowledges in writing that they are responsible for the security of Company cardholder data that Vendor possesses or otherwise stores, processes, or transmits on behalf of Vendor and will furnish evidence of current PCI-DSS certification for the relevant services. Vendor will conduct PCI-DSS required quarterly network scans on the in-scope environment via an Approved Scanning Vendor (as defined by PCI-DSS), whose use is hereby consented to by Company. To the extent that Vendor is performing Services that are “in scope” of Payment Card Industry standards (PCI Service Provider or Merchants) acting on behalf of Company must have their PCI scope assessed by a Qualified Security Assessor (QSA) with an annual Report of Compliance (ROC). Vendor shall provide upon request and on a defined rolling basis, evidence of compliance (i.e. an Attestation of Compliance, Certificate of Compliance, etc.).

16. **Data Backup.** Vendor will employ a business continuity plan covering all Services and Company Confidential Information that ensures (a) all Personal Information and Restricted Information in Vendor’s custody or control is backed up and segregated from production environments at least daily; (b) all non-Personal and Restricted Confidential Information is similarly backed up and segregated from production environment at a reasonable frequency given the nature of the Services and the sensitivity of the information; and (c) that any disrupted Vendor Services will be restored to functionality no later than 24 hours after the disruption. Further, any Company Confidential Information no longer necessary for the performance of Services will, unless otherwise required by law, be securely deleted / destroyed by whichever time comes first: (i) termination of the Agreement pursuant to Section 10.8 (Treatment of Confidential Information Following Termination) of the Agreement; (ii) Vendor’s record retention schedule; (iii) as documented in an applicable SOW or (iv) Company’s reasonable request.

17. **Materiality.** If Vendor fails to comply with this Exhibit, Company may suspend Vendor’s performance under the Agreement or terminate the Agreement with immediate effect. Any suspension or termination will be without any penalty, liability or further obligation and without prejudice to any other rights Company might have under the Agreement.
Privacy Requirements

This Privacy Requirements Exhibit ("Exhibit") is an attachment to and incorporated into the Agreement. In the event of a conflict between this Exhibit and any other terms of the Agreement (including but not limited to any attachment, statement of work, order, exhibit, referenced URL, etc.), the language that is more protective of Company and Company Confidential Information shall govern. Capitalized terms used but not defined herein will have the meanings set forth in the Agreement.

1. **Scope of Agreement.** Vendor will comply with the provisions of this Exhibit ("Privacy Requirements") if Vendor accesses, collects, stores, transmits, discloses, processes, and/or otherwise uses Personal Information ("Use").

2. **Personal Information.** Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household. Personal Information obtained by Vendor independent of the Agreement is not considered Personal Information for the purposes of this Exhibit unless it is used for or in connection with the Services in some capacity.

3. **Processing.** Vendor will process Personal Information on behalf of Company as described in the applicable Statement of Work or Order. The processing activities are as described in the applicable Statement of Work or Order.

4. **Administration.** Consistent with the size and complexity of its organization, Vendor will maintain its own privacy program that manages its handling of Personal Information and includes a documented data breach response. Vendor will appoint (or have appointed) a leader to oversee this privacy program. Where necessary, Vendor will assist Company in completing privacy impact assessments and consultations with the relevant supervisory authorities.

5. **Ownership.** As between the parties, all Personal Information is and remains the property of Company regardless of what party has custody of such information.

6. **Usage.** Vendor will only Use in accordance with Company's instructions and never in a manner that violates Law or fails to meet the requirements set forth in this Exhibit. Vendor will not distribute, sell, license, lease, transfer, or otherwise convey Personal Information on each occasion, without Company’s prior written consent.

7. **Collection.** To the extent Vendor collects Personal Information on Company's behalf, Vendor will only collect that Personal Information necessary to perform its Vendor contracted services or to otherwise fulfill Company's instruction on collection. Vendor will not collect Personal Information online from individuals under the age of 16 or knowingly provide Company with Personal Information collected from individuals under the age of 16 without Company prior written consent and instruction.

Vendor will notify Company about the methods of operation and data collection capabilities for any cookie, Javascript, pixel, beacon, statistical ID, probabilistic ID, UDID, similar tracking mechanism(s) or other method of monitoring a user or device across web and/or app locations or properties ("Tracking Technologies"). Vendor will not use such Tracking Technologies without Company’s prior written consent. Vendor will never use Tracking Technologies that: (i) use Flash local shared objects, (ii) fail to provide users with an opportunity to control the use of such Tracking Technologies, (iii) are deployed on behalf of other parties (so-called "fourth party" tracking or “piggybacking”), or (iv) circumvent user preferences as designated in Web browser privacy controls.

8. **Data Location.** Unless otherwise agreed upon by the parties, Vendor will collect, store, transmit, disclose, process and Use Personal Information only in the United States.
9. Legal Compliance.
   a. Vendor will, and will cause any person or entity acting on its behalf, to fully comply with all
      applicable governmental, legal, regulatory and professional requirements relating to privacy.
   b. Vendor will handle all Personal Information of individual state residents in accordance with
      their respective state privacy statutes and regulations, including Massachusetts Code of
      Regulations, 201 CMR §§ 17.00 et. Seq., California Consumer Privacy Act, etc., as
      applicable.
   c. If Vendor has access to “protected health information” (as such term is defined by the HIPAA
      Privacy Rule) then Vendor will notify Company and enter into a Business Associate
      Agreement (“BAA”) in a form that meets minimum legal requirements and is mutually
      acceptable to the parties.

10. Data Subject Rights. Where possible and to the extent relevant, Vendor shall put in place
    technical and organizational measures to enable Company to comply with its obligations to
    respond to requests from data subjects to exercise their rights in respect of their Personal
    Information, including but not limited to the right to access the Personal Information processed by
    Company and to request the rectification of inaccurate Personal Information. Vendor shall not
    respond to any such request from a data subject without receiving the prior written consent of
    Company.

11. Vendor Privacy Policies. By execution of the Agreement, Vendor is attesting that: (i) it has
    established general privacy policies and procedures that comply with all material requirements of
    Laws and (ii) its current practices are in compliance with the policies and procedures as
    described herein.