Data Privacy and Cyber Security Terms and Conditions

In the regular course of business, Company collects and maintains information that identifies or could be used to identify individuals (e.g., employees, applicants, business or prospect contacts, or royalty owners), which may include data such as a person's Social Security number, driver's license number, bank account or credit card information, health information, employment-related information, or login and password credentials (all such data pertaining to identified or identifiable individuals, whether or not specifically listed, being "Personal Information").

In connection with the Work, Contractor may have access to, receive, generate, handle, store, transmit, or otherwise process Personal Information or other confidential or proprietary materials, information, or data maintained by or concerning Company, including, without limitation "Confidential Information" or "Proprietary Information," to the extent those terms are defined in the Commercial Agreement (collectively with Personal Information, "Company Information"), and Contractor may have access to and/or custody or control of computing equipment, systems, applications, and software used by or for Company to process Company Information ("Company Systems").

Accordingly, Contractor agrees as follows:

1. Contractor is responsible for the security of Company Information that it receives or accesses in performing Work, and Contractor shall at all times maintain appropriate information-security measures with respect to Company Information in a manner consistent with applicable law.

2. Contractor must implement and maintain current and appropriate administrative, technical, and physical safeguards, with respect to all business processes and physical premises and all computing equipment, systems, applications, and software used by or for Contractor to access any Company Systems or to access, receive, generate, handle, store, transmit, or otherwise process any Company Information (such equipment, systems, applications, and software, "Contractor Systems"), to protect against unauthorized use of, unauthorized access to, damage to, or unplanned unavailability of such Company Systems or such Company Information (any such use, unavailability, access, or damage, a "Security Incident"). At a minimum, such safeguards shall be consistent with generally-recognized best practices for physical security, computing systems security, and information security. Without limiting the foregoing, unless otherwise agreed in writing as to Company Information that Company deems to be non-sensitive, Contractor must appropriately and effectively encrypt (i) Company Information transmitted over the Internet, other public networks, or wireless networks; and (ii) Company Information stored on laptops, tablets, or any other removable or portable media or devices. In addition, Contractor shall regularly screen for and remove software or computer code designed to perform an unauthorized function on, or permit unauthorized access to, an information system, including without limitation, computer viruses, Trojan horses, worms, spyware, and time or logic bombs from Contractor Systems, and Contractor shall apply available security updates and patches to Contractor Systems promptly and on an ongoing basis.

3. Contractor must identify to Company all subcontractors, consultants, and other persons not directly employed by Contractor who may have access to Company Information or Company Systems in connection with the Work. Before Contractor permits any subcontractor, consultant, or other person not directly employed by Contractor to have access to Company Information or Company Systems, Contractor must obtain Company's written approval, not to be unreasonably withheld Contractor must restrict the Company Information or component of Company Systems to which a given employee or subcontractor has access to only that Company Information or component of Company Systems which such employee or subcontractor needs to access in the course of such employee's or subcontractor's duties and responsibilities in connection with the Work.

4. Before granting access to Company Information or Company Systems, Contractor must ensure that its employees agree and each subcontractor agrees to abide by these information security measures (or other applicable measures that are at least as protective of Company Information and Company Systems). Contractor shall be responsible for the acts and omissions of its employees and subcontractors under this Addendum as though such acts or omissions were those of Contractor.

5. Absent Company's advance written permission, Company Information must not be stored, accessed, or processed at any location outside of the United States or its territories.

6. Contractor has no rights in the Company Information or any Company Systems other than the rights Company grants to Contractor to provide the Work. Contractor may not use Company Information or any Company Systems for purposes other than performing the Work, and Contractor must ensure that its subcontractors are restricted from any use of Company Information or Company Systems other than for purposes of performing the Work. Except to the extent otherwise expressly permitted under the Commercial Agreement, Contractor and its subcontractors may not disclose Company Information other than to the extent required by law or a governmental authority having jurisdiction over Contractor or its subcontractor, as applicable. In the event of such required disclosure, Contractor must notify Company in advance (if legally permissible to do so) of any such required disclosure and must reasonably cooperate with any decision by Company to seek to condition, minimize the extent of, or oppose such disclosure.

7. Contractor will immediately notify Company if Contractor discovers any actual or reasonably suspected Security Incident. In no event shall Contractor's notification to Company be later than three (3) calendar days after Contractor discovers the Security Incident; provided, however, that more immediate notification shall be given as the circumstances warrant or if more immediate notification is required by law. Contractor must provide all necessary and reasonable cooperation with respect to the investigation of such Security Incident, including the exchange of pertinent details (such as access records and log files). In addition, Contractor must promptly undertake appropriate remediation measures with respect to Contractor Systems involved, and shall inform Company on an ongoing basis regarding the same.

8. Subject to requirements of data security or privacy laws, Company will determine how, whether, and when to provide notice of a Security Incident that involves Personal Information to (a) any individuals whose personal information has been actually or potentially compromised; (b) any governmental authority; and/or (c) any other entity, including, but not limited to, consumer credit reporting agencies or the media. If the Security Incident involves Company Information in Contractor's custody or control (including in the custody or control of any of Contractor's subcontractors) or is accomplished using access permissions or credentials extended to Contractor, then: (x) if the Security Incident involves Personal Information, (i) Contractor must reimburse Company for costs or expenses Company incurs in connection with notices described in the preceding sentence (including the provision of credit monitoring or other identity protection services, to the extent the provision of such services is legally required or customary for similar data security incidents, and (ii) Contractor shall indemnify and hold Company harmless from all claims, costs, expenses, and damages (including reasonable attorneys' fees) that Company incurs in connection with any third-party claim or regulatory action arising from the Security Incident, and (y) if the Security Incident involves confidential or proprietary information of a third party for which Company is liable or accountable pursuant to any contractual or legal theory, then Contractor shall indemnify and hold Company harmless from all claims, costs, expenses, and damages (including reasonable attorneys' fees) that Company incurs in connection with a claim by or on behalf of such third party arising from the Security Incident. In addition, if the Security Incident involves damage to Company Systems or unplanned unavailability of any Company Information or Company Systems as a result of any act or omission of Contractor (including any act or omission of Contractor's subcontractors), then Contractor must reimburse Company for costs or expenses Company incurs in connection with containing, mitigating, and remediating such damage or unavailability. All notices and other public communications about any Security Incident must be approved by Company in writing before they are distributed.

9. Contractor must comply with one or both of the following, as determined by Company:

   a. On an annual or more frequent basis, Contractor must, at its expense, engage a qualified, independent third-party security professional to audit the security of the Contractor Systems and the business processes used by or for Contractor to access any Company Systems or to access, store, process, or transmit any Company Information. Such audit shall be performed according to ISO/IEC 27001 standards, and must be accompanied by a report. Such report, which shall be provided to Company upon request, must include a clear description of the scope of the audit and any material findings by the auditor.

   b. Each calendar year, Contractor must provide to Company a current Type 2 Service Organizations Control (SOC) report or comparable report satisfactory to Company, confirming the adequacy of Contractor's controls under the Trust Work Principles and Criteria of the American Institute of CPAs, or comparable principles and requirements satisfactory to Company. The scope of each report must include the Contractor Systems and the business processes used by or for Contractor to access any Company Systems or to access, store, process, or transmit any Company Information, and each report must include a list of the controls that were tested.

10. Subject to any legitimate confidentiality, contractual, and security concerns and limitations that cannot be addressed by an appropriate non-disclosure agreement and reasonable access screening measures, Contractor must cooperate and permit Company or its representative (and any governmental authorities with jurisdiction in connection with an audit request concerning Company) reasonable access to Contractor's premises, the premises of any approved subcontractor, and all pertinent security procedures and physical access controls and records in order to verify Contractor's compliance with its obligations under this Privacy and Cyber Security Addendum and with respect to any other privacy, confidentiality, and security provisions in the Commercial Agreement. Contractor must obtain a contractual right of access in its contracts with any subcontractors that is sufficient to permit access by Company pursuant to the preceding sentence.

11. Notwithstanding anything to the contrary in the Commercial Agreement, Company may terminate the Commercial Agreement without penalty or fee at any time upon thirty (30) days written notice if Company determines (as a result of a Security Incident, based upon on-site reviews or review of audit findings, based upon reviews of SOC or comparable reports, or otherwise) that Contractor has failed to abide by the requirements in this Addendum

or that Contractor has not demonstrated it is capable of and committed to doing so.

12. Whenever Company Information is no longer needed for the performance of Work, or at any time upon written notification from Company, Contractor must unconditionally and without any charge or fee return or, at Company's written election, certify the secure destruction of, all Company Information in Contractor's custody or control (including Company Information in the custody or control of any of Contractor's subcontractors) save and except for any Company Information as to which return or destruction is not technically feasible and which will be securely destroyed in the normal course of Contractor's record retention program. Whenever access to Company Systems is no longer necessary for the performance of Work, or at any time upon written notification from Company, Contractor shall unconditionally cease and discontinue access to Company Systems and shall unconditionally and without any charge or fee return any Company Systems that are in Contractor's custody or control.

13. With respect to all Company Information that constitutes payment cardholder information under the Payment Card Industry Data Security Standard ("PCI DSS") and with respect to any actions or activity that may impact the security of Company's systems securing payment cardholder information, Contractor must, and must cause its approved subcontractors, as applicable, to:

a. abide by PCI DSS, as updated from time to time (currently, version 3.2), and related security and reporting requirements or standards imposed by applicable payment card brand(s) including through the provision of, preparation of, or cooperation in connection with any all reports, assessments, audits, inquiries, or attestations made, to be made, or desired by Company pursuant to PCI DSS or applicable payment card brand requirements or standards;

b. annually, and at such other times as Company may reasonably request, provide Company with a certification demonstrating compliance with PCI DSS in the relevant capacity, without charging Company any fee or other amount with respect to such compliance or certification thereof; and

c. without limiting the foregoing, refrain from any recording or storage of card security codes, render primary account numbers unreadable wherever stored, and dispose of payment cardholder information in compliance with PCI DSS Requirement 9.8.

14. If the Commercial Agreement contemplates access to or the handling of any information that constitutes "Protected Health Information" under the Health Insurance Portability and Accountability Act and regulations adopted thereunder ("HIPAA"), the Parties must enter into a separate Business Associate Agreement that complies with HIPAA before Contractor will be granted access to any Protected Health Information.

15. Notwithstanding anything in the Commercial Agreement to the contrary: (a) this Addendum shall remain in effect as to Company Information for so long as such Company Information remains in the custody or control of Contractor (including any of its subcontractors), and (b) this Addendum shall remain in effect as to Contractor's access to or custody or control of Company Systems for so long as such Company Systems remain accessible by Contractor (including any subcontractor) and/or remain in Contractor's custody or control.