Information Security Requirements

Introduction.

These Information Security Requirements are contractual obligations under contractors, consultants, suppliers and vendors (collectively, "Suppliers") agreement(s) between Supplier and Prudential (the "Agreement(s)"), or any obligations under applicable law. The more restrictive obligations and requirements shall apply to the extent of any conflict between any of the foregoing and these Information Security Requirements. These Information Security Requirements are not intended to replace Supplier's standard security practices but are intended to address the minimum controls that Supplier must have in place. Any capitalized terms not defined herein shall have meaning ascribed to it the Agreement to which these Information Security Requirements relate.

Information Security Program.

- Supplier will ensure that (i) its treatment of Confidential Information is in compliance with applicable laws and regulations with respect to privacy and data security, and (ii) it has implemented and currently maintains an effective written information security program ("Information Security Program") that includes administrative, technical, and physical safeguards and other security measures necessary to (a) ensure the security, confidentiality, and integrity of Confidential Information; (b) protect against any anticipated threats or hazards to the security, confidentiality, and integrity of Confidential Information; (c) protect against unauthorized access to, destruction, modification, loss, disclosure or use of Confidential Information; and (d) detect and respond to security incidents involving Confidential Information. Supplier will notify Prudential of its designated primary security manager. The security manager will be responsible for managing and coordinating the performance of Supplier's obligations set forth in its information security program and in this Agreement.
- In addition, Supplier's Information Security Program shall address the following areas: (a) risk assessment and identification; (b) data governance and classification; (c) asset inventory and device management; (d) access controls and identity management; (e) business continuity and disaster recovery planning and resources; (f) system operations and availability; (g) systems and network monitoring and security, including anti-virus and malware protection; (h) system and application development and quality assurance; (i) physical security and environmental controls; (j) vendor management; and (k) training.
- Supplier shall review and, as appropriate, revise its Information Security Program at least annually or whenever there is a material change in Supplier's business practices that may reasonably affect the security, confidentiality or integrity of Confidential Information. During the course of providing the services, Supplier may not alter or modify its Information Security Program in such a way that will weaken or compromise the security, confidentiality, or integrity of Confidential Information. Supplier must notify Prudential when it revises its Information Security Program. Supplier shall immediately notify Prudential if Supplier is in material breach of this Section. At Prudential's request, Supplier agrees to certify in writing to Prudential, its compliance with the terms of this Section.
- Supplier shall encrypt, using industry standard encryption tools, all Confidential Information that Supplier: (a) transmits or sends wirelessly or across public networks; (b) stores on laptops or storage media; (c) where technically feasible, stores on portable handheld devices (e.g.,

smartphones, tablets, or similar devices); and (d) stores on any device that is transported outside of the physical or logical controls of Supplier. Supplier will safeguard the security and confidentiality of all encryption keys associated with encrypted Personal Information.

- Supplier shall maintain appropriate access controls, including, but not limited to, limiting access to Confidential Information to the minimum number of Supplier Employees who require such access in order to provide the services to Prudential. Supplier shall periodically review and update such access privileges.
- Supplier shall conduct periodic risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Confidential Information. Based on such assessments, Supplier shall evaluate and improve, where necessary, the effectiveness of its Information Security Program and information security controls. Such assessments will also consider Supplier's compliance with its Information Security Program and the laws applicable to Supplier.
- Supplier shall conduct the following testing:

    - At least quarterly, Supplier shall (1) scan internal systems and other information resources including, but not limited to, networks, servers, applications and databases, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities, ensure that such systems and other resources are properly hardened, and identify any unauthorized wireless networks; and (2) scan externally-facing systems and other information resources, including but not limited to, networks, servers and applications, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities;

    - Supplier shall conduct internal and external penetration testing at least annually;

    - If any scanning and/or testing detects any anomalies, intrusions, or vulnerabilities in any systems or other information resources processing, storing or transmitting any of Prudential's Confidential Information, Supplier shall promptly report those findings to Prudential.

Security Incidents. Supplier shall notify Prudential, promptly and without unreasonable delay, but in no event more than 48 hours of learning of any: (a) unauthorized access or disclosure, unauthorized, unlawful or accidental loss, misuse, destruction, acquisition of, or damage to Confidential Information may have occurred or is under investigation; or (b) act or attempt to gain unauthorized access to, disrupt, or misuse an information system that handles or stores Confidential Information (either, a "Security Incident"). Thereafter, Supplier shall:

- take all steps to mitigate or contain the Security Incident. To the extent that a Security Incident resulted from a violation of Supplier's duties under this Agreement, Supplier will (i) assist with curing any alleged violation and ensure that no further violations shall occur; and (ii) provide Prudential with a written statement confirming such cure and no further violations;

- promptly furnish to Prudential full details of the Security Incident, which shall include the estimates of the effects on Prudential and specify any correction action to be taken by Supplier;

- assist and cooperate with Prudential or Prudential's designated representatives in Prudential's investigation of Supplier, Employees or third parties related to the Security Incident. Supplier will provide Prudential with physical access to the facilities and operations affected, facilitate Prudential's interviews with Employees and others involved in the matter, and make available to Prudential all relevant records, logs, files, and data;

- cooperate with Prudential in any litigation or other formal action against third parties deemed necessary by Prudential to protect Prudential's rights; and

- take appropriate action to prevent a recurrence of any Security Incident.

In addition to the foregoing, Supplier agrees that in the event of a Security Incident, Prudential has the sole right to determine: (i) whether notice is to be provided to any individuals, regulators, consumer reporting agencies, or others as required by law or regulation, or in Prudential's discretion; and (ii) the contents of each notice, whether any type of remediation will be offered to affected persons, and the nature and extent of the remediation. Any such notice or remediation shall be at Supplier's sole cost and expense. Unless required by law, Supplier shall not notify any individual or any third party other than law enforcement of any potential Security Incident involving Confidential Information without first consulting with, and obtaining the permission of, Prudential.

Ver. October 11, 2023