Supplier Security Requirements

Supplier shall implement and maintain all appropriate technical and organizational security measures to protect from a Security Incident and to preserve the security, integrity and confidentiality of all Personal Information processed under or in connection with the Agreement(s). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. At a minimum, Supplier agrees to the following security measures:

Physical Controls. Supplier will maintain physical controls designed to secure relevant facilities, including layered controls covering perimeter and interior barriers, individual physical access controls, strongly-constructed facilities, suitable locks with key management procedures, access logging, and intruder alarms/alerts and response procedures.

Technical Controls.

Supplier shall:

- establish and enforce access control policies and measures to ensure that only individuals who have a legitimate need to access Personal Information will have such access, including multi-factor authentication;
- promptly terminate an individual's access to Personal Information when such access is no longer required for performance under the Agreement;
- maintain reasonable and up-to-date anti-malware, anti-spam, and similar controls on Supplier's networks, systems, and devices;
- log the appropriate details of access to Personal Information on Supplier's systems and equipment, plus alarms for attempted access violations, and retain such records for no less than 90 days;
- maintain controls and processes designed to ensure that all operating system and application security patches are installed within the timeframe recommended or required by the issuer of the patch;
- implement reasonable user account management procedures to securely create, amend, and delete user accounts on networks, systems, and devices through which Supplier accesses Personal Information, including monitoring redundant accounts and ensuring that information owners properly authorize all user account requests; and
- have the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident.

Personnel Security. Supplier will maintain personnel policies and practices restricting access to Personal Information, including having appropriate use guidelines, written confidentiality agreements, and performing background checks in accordance with Applicable Laws on all personnel who Process Personal Information or who implement, maintain, or administer Supplier's security measures.

Training and Supervision. Supplier must provide ongoing privacy and information security training and supervision for all Supplier personnel who Process Personal Information.

Encryption Requirements. All Personal Information shall be encrypted at all times (at rest and in transit) while in Supplier's possession or control. All encryption shall be in accordance with industry standards, including NIST SP 800-57, and including at a minimum:

Encryption at rest and in transit of all Personal Information and any backup media containing Personal Information with:

- Industry best standard encryption algorithm (e.g. AES-256, RSA, WPA-2);
- Transport Layer Security "TLS" v1.2 or higher during transmission;
- Full disk encryption of removable media (e.g. USB drives, mobile devices, CD/DVD-ROMS, portable hard drives, etc.) or any laptops, smartphones, tablets, or other portable devices (collectively, "Portable Devices") using an encryption algorithm that meets or exceeds industry best practices; and

- Digital certificates signed by a trusted certificate authority.

Key management policies and procedures for secure generation, storage, access, distribution, archiving, recovery, and destruction.

Use of Canary Networks, Systems, or Devices. To the extent that Supplier accesses

Canary-owned or Canary-managed networks, systems, or devices (including Canary APIs,

corporate email accounts, equipment, or facilities) to access Personal Information, Supplier must comply with Canary's written instructions, system requirements, and policies made available to Supplier.

System Acquisition, Development, and Maintenance. If Supplier develops software for use by Canary and/or Canary clients or for use in Processing Personal Information, Supplier must adhere to industry best practices and standards for Secure Software Development Lifecycle (SSDLC), including all of, but not limited to, the following techniques:

- Consistently executed secure code reviews and testing either through manual peer review or via a code scanning solution;
- Leveraging security guidelines from one or all of the following industry best practices and standards – OWASP Top 10, SANS Top 25 and Cloud Security Alliance;
- Protection of test data and content and removal of test data and content before deployment to production;
- System acceptance testing; and
- System change control and approvals before deployment to production.

Public Cloud Services. If Supplier uses a public cloud service, Supplier must apply industry best practices for cloud management including:

- enforce MFA for all administrative users of Supplier cloud services;
- separation of cloud environments to include strong key management practices that separate and prevent access to Personal Information from other Supplier and Supplier customer users, as well as logical separation from other data and content; and
- use industry standard encryption to protect all Personal Information when transmitted over all networks to, from, and within a public cloud service; and stored withing a public cloud service.

PCI Compliance. To the extent Supplier Processes any Cardholder Data for or on behalf of Canary, Supplier will at all times meet or exceed all Applicable Laws related to the collection, storage, accessing, and transmission of such data, including those established by Payment Card Industry Data Security Standards. The Payment Card Industry Data Security Standards are currently published at the following URL https://www.pcisecuritystandards.org/.

Destruction; Sanitization.

Return or Deletion of Information. Upon the termination or expiration of the Agreement for the Services, Supplier will promptly return to Canary all copies, whether in written, electronic or other form or media, of Personal Information in Supplier's possession or the possession of Sub-Processor; where permitted delete and render Personal Information unreadable in the course of disposal, securely dispose of all such hard copies, and where requested certify in writing Supplier's compliance.

Sanitization. Supplier will use a media sanitization process that deletes and destroys data in accordance with the US Department of Commerce's National Institute of Standards and Technology's guidelines in NIST Special Publication 800-88 or equivalent standard.

Endpoint Security Requirements.

Supplier must maintain the following endpoint security requirements: patch management; full disk encryption; remote wipe capability in case of lost/stolen laptop; anti-malware; inactivity timeout, (e.g. screen saver lock); and complex passwords of at least 8 characters.

The storage or transmission of Personal Information on or through removable media (e.g. USB drives, mobile devices, CD/DVD Roms, etc.) is strictly prohibited.

Business Continuity and Disaster Recovery.

Business Continuity Plan. Supplier shall have a current Business Continuity Plan ("BCP"). Canary reserves the right to review a summary of the items included in the BCP. Supplier shall ensure that there is a person appointed by Supplier and charged with the responsibility of developing and maintaining the BCP. The BCP must be updated annually. Current test results of BCP testing must be retained until the next testing occurrence has been completed.

Disaster Recovery. Supplier shall have documented disaster recovery plans, provisioning and tested disaster recovery capabilities in place which can recover within an acceptable amount of time those critical functions/ services for which Canary has contracted, and restore connectivity from Supplier's recovery site to Canary. In keeping with industry standards and best practices, Supplier plans shall be reviewed and successfully tested at a minimum annually. Supplier shall make available, upon request, a summary of the most current test report for systems or critical business process utilized in support of Canary with summary of corrective actions accomplished for any identified substantive plan or provisioning shortfalls discovered in the testing process.

Assessments; Audits; Corrections.

Canary's Security Assessment. On Canary's written request Supplier will promptly and accurately complete Canary's written privacy and security questionnaire regarding any network, application, system, or device, or security measures applicable to Supplier's access to Personal Information. Supplier will provide any additional assistance and cooperation that Canary may reasonably require during any assessment of Supplier's security measures, including providing Canary with reasonable access to personnel, information, documentation, infrastructure and application software, to the extent any of the foregoing is involved in Supplier's access to Personal Information.

Audits and Certifications; Regulatory Audits.

Audits and Certifications. Upon request by Canary, Canary may conduct an audit of Supplier's architecture, systems and procedures relevant to the protection of Personal Information at locations where Personal Information is Processed. Supplier will work cooperatively with Canary to agree on an audit plan in advance of any audit. Provided, however, if the scope of the audit is addressed in a SSAE 16/SOC1, SOC2, ISO 27001, NIST, PCI DSS, HIPAA or similar audit report performed by a qualified third party auditor within the prior twelve (12) months, and Supplier confirms there are no known material changes in the controls audited, Canary may agree to accept those reports in lieu of requesting an audit of the controls covered by the report.

Regulatory Audit. Notwithstanding Section (i)(b) if a Regulator requires an audit of the data processing facilities from which Supplier process Personal Information in order to ascertain or monitor Canary's compliance with Applicable Law, Supplier will cooperate with such audit.

Supplier's Continuous Self-Assessment; Penetration Testing. Supplier will continuously monitor risk to Personal Information and ensure that the security measures are properly designed and maintained to protect the confidentiality, integrity, and availability of Personal Information. At least one time each year during the term of the Agreement, Supplier will retain, at its sole cost and expense, an independent third party to conduct a penetration test of Supplier's infrastructure designed to detect any material security weaknesses in such infrastructure. Supplier will use a reputable third party to conduct such testing that is certified by recognized industry standards as being qualified to perform such penetration testing. Supplier will reasonably discuss the results of such testing with Canary in a general nature so as not to expose any potential vulnerabilities to broader disclosure and, to the extent any such material weakness is found, will take appropriate action, prompt under the circumstances, to remedy such weakness.