SUPPLIER DATA PROTECTION ADDENDUM (“DPA”)

This Data Protection Addendum (“DPA”) is entered into by and between Canary LLC, a California limited liability company located at 2700 Camino Ramon, Suite 110 San Ramon CA 94583 (“Canary”) and the party (including any personnel, contractor, or agent acting on behalf of such party) that performs Services for Canary under the Agreement (“Supplier”).

BACKGROUND

Canary and Supplier have entered into one or more purchase orders, contracts, and/or agreements (“Agreement(s)”) that may require Supplier to process Personal Information provided by Canary. This DPA forms part of the Agreement(s) and/or other services agreement(s) between Canary and Supplier.

To comply with Data Protection Law (defined below), Canary must ensure the appropriate protection of all Personal Information when Canary engages third party Suppliers. Accordingly, this DPA sets out the additional terms, requirements and conditions on which Supplier will obtain, handle, process, disclose, transfer, or store Personal Information when providing services under the Agreement.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION.
    1. **Definitions**.
    2. Capitalized terms used but not defined in this DPA will have the meanings otherwise set forth in the Agreement. For purposes of this DPA, the following terms will have the meaning ascribed below:
        1. “Data Protection Law” means all applicable federal, state, and foreign laws, directives, and regulations relating to the Processing, protection, security or privacy of Personal Information, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, the California Consumer Privacy Act (“**CCPA**”) (Cal. Civ. Code §§1798.100 *et seq.*), the General Data Protection Regulation, Regulation (EU) 2016/679 (“**GDPR**”), equivalent requirements in the United Kingdom including the UK General Data Protection Regulation and the Data Protection Act 2018 (“**UK Data Protection Law**”), and the Swiss Federal Act on Data Protection (“**FADP**”).
        2. “**Cardholder Data**” means any primary account number, cardholder name, expiration date and/or service code, and security-related information (including but not limited to card validation codes/values, full track data, PINs and PIN blocks) used to authenticate cardholders or authorize payment card transactions.
        3. “Data Subject” means an identified or identifiable natural person about whom Personal Information relates.
        4. “Personal Information” means any information Supplier processes for Canary that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Supplier's possession or control or that Supplier is likely to have access to, or (b) the relevant Data Protection Law otherwise define as protected Personal Information. Personal Information includes names, email addresses, postal addresses, telephone numbers, payment card information, online identifiers (including IP addresses and cookie identifiers).
        5. “Processing” or “Process” means either any activity that involves the use of Personal Information or as the relevant Data Protection Law may otherwise define processing, or process. It includes obtaining, recording or holding the Personal Information, or carrying out any operation or set of operations on the Personal Information including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring

Personal Information to third parties.

6. **"Secondary Use"** means Processing Personal Information for purposes other than as necessary to fulfill the Agreement and comply with the specific instructions stated in the Agreement, or for any purpose that would be a considered a "sale" of Personal Information as defined by the CCPA.

7. "Security Incident" means any accidental or unlawful destruction, loss, or alteration of Personal Information, or any unauthorized access to, or use or disclosure of, Personal Information.

8. **"Services"** means the services provided by Supplier to Canary under and as more particularly described in the Agreement(s).

9. **"Subprocessor"** means any third party (including any Supplier affiliates) engaged directly or indirectly by Supplier to process any Personal Information relating to this DPA and/or the Agreements. The term "Subprocessor" shall also include any third party appointed by a Subprocessor to process any Personal Information relating to this DPA and/or the Contract(s). Subprocessor includes "Subprocessor" within the meaning of Standard Contractual Clauses.

10. **"Supplier"** means the party (including any personnel, contractor, or agent acting on behalf of such party) that performs Services for Canary under the Agreement.

3. **Supplemental Terms.** The Attachments form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Attachments.

4. **Order of Precedence.** In the case of conflict or ambiguity between: (a) any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail; and (b) any of the provisions of this DPA and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

2. ROLE AND SCOPE OF PROCESSING.
    1. **Relationship of the Parties**.
        1. Canary and Supplier acknowledge that for the purpose of Data Protection Law, Canary is the Controller and Supplier is the Processor. Supplier shall process Personal Information under the Agreements only as a Processor acting on behalf of Canary (whether as Controller or itself a Processor on behalf of a third party Controller). Each party shall comply with its obligations under Data Protection Law.

        2. For the purposes of the CCPA (to the extent the CCPA is applicable), Canary is a "business" and Supplier is a "service provider". Supplier, as service provider, will not (a) sell Canary Personal Information, or (b) retain, use, or disclose Canary Personal Information for any purposes other than for performing Supplier's obligations under the Agreement. The Parties agree that Canary's transfer of Personal Information to Supplier is not a sale, and Supplier provides no monetary or other valuable consideration to Canary in exchange for Canary Personal Information. Supplier certifies that it understands the restrictions set out in this Section 2.1 and will comply with them.

    2. **Details of Personal Information Processing**. Attachment 1 to this DPA sets out a description of the Personal Data as required by Data Protection Law.

    3. **Limited Use**. Supplier will only Process the Personal Information to the extent, and in such a manner, as is necessary to provide the Services in accordance with Canary's instructions. Supplier will not process the Personal Information for any other purpose or in a way that does not comply with this DPA or the Data Protection Law.

4. **Confidentiality and Non-Disclosure**. Personal Information will be deemed Canary's Confidential Information under the Agreement. Supplier will ensure that persons authorized by Supplier to Process any Personal Information are subject to appropriate confidentiality obligations. Supplier will maintain the confidentiality of all Personal Information and will not disclose Personal Information to third parties unless Canary or this DPA specifically authorizes the disclosure, or as required by law. If a law requires Supplier to process or disclose Personal Information, Supplier must first inform Canary of the legal requirement and give Canary an opportunity to object or challenge the requirement, unless the law prohibits such notice.

5. **Return or Disposal**. At Canary's request, Supplier will give Canary a copy of or access to all or part of Canary's Personal Information in its possession or control in the format and on the media reasonably specified by Canary. On termination of the Agreement for any reason or expiry of its term, Supplier agrees to delete and securely erase or, if directed in writing by Canary (which may be delivered via email), return and not retain, all or any Personal Information related to this agreement in its possession or control.

3. SECURITY.
    1. **Security Measures**. Supplier must at all times implement and maintain reasonable and appropriate physical, technical and organizational security measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display or distribution, and against accidental loss, destruction or damage including, but not limited to, the minimum security measures set out in Attachment 2.

    2. **Security Assistance**. Taking into account the nature of Processing and the information available to the Supplier, Supplier will assist Canary in ensuring compliance with its security obligations under Data Protection Law, including Article 32 of the GDPR and Article 32 of the UK GDPR.

4. SECURITY INCIDENT.
    1. **Security Incident Response Program**. Supplier must maintain a reasonable Security Incident response program.

    2. **Security Incident Notification**.
        1. If Supplier becomes aware of any unauthorized or unlawful processing of the Personal Information or any Security Incident, Supplier will immediately, and without undue delay:
            1. stop the unauthorized access;

            2. secure the Personal Information;

            3. notify Canary (in no event more than 24 hours after the discovery of the Security Incident) by sending an email to security@canarymarketing.com with the information described in Subsection (b) below. This notification is required even if Supplier has not conclusively established the nature or extent of the Security Incident; and

            4. assist Canary in complying with its Security Incident notification or cure obligations under applicable laws and as otherwise reasonably requested.

        2. Where the Supplier becomes aware of any Security Incident, it shall, without undue delay, provide Canary with timely and sufficient information to allow Canary to meet any obligations under Data Protection Law. This includes, but is not limited to:
            1. a description of the Personal Information subject to the Security Incident (including the categories and number of data records and Data Subjects concerned) and the likely consequences of the Security Incident;

            2. the date and time of the Security Incident;

            3. a description of the circumstances that led to the Security Incident (e.g., loss,

theft, copying);

4. a description of the measures Supplier has taken and proposes to take to address the Security Incident; and

5. relevant contact people who will be available until the parties mutually agree that the Security Incident has been resolved.

3. **Remediation; Investigation**. In the event of a Security Incident, Supplier shall, at Supplier's cost, take appropriate steps to promptly remediate the root cause(s) of any Security Incident, and will fully co-operate with Canary in Canary's handling of the matter . Furthermore, Supplier shall take such measures and actions as are directed by Canary (or as appropriate) to assist in the investigation, mitigation, and remediation of each such Security Incident, and shall keep Canary up-to-date about all developments in connection with the Security Incident.

4. **No Unauthorized Statements**. Except as required by applicable laws, Supplier will not make (or permit any third party to make) any statement concerning the Security Incident that directly or indirectly references Canary or any of Canary's clients, unless Canary provides its explicit written authorization.

5. **Security Incident Assistance**. Taking into account the nature of Processing and the information available to the Supplier, Supplier will assist Canary in ensuring compliance with Canary's notification obligations under Data Protection Law in connection with any Security Incident, including in ensuring compliance with Canary's obligations pursuant to Articles 33 and 34 of the GDPR and Articles 33 and 34 of the UK GDPR.

5. CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION.

1. Supplier shall, at all times, provide an adequate level of protection for the Personal Information, wherever Processed, in accordance with the requirements of the applicable Data Protection Law.

2. **Personal Information Originating from the UK, EEA or Switzerland**. If Personal Information originates from the UK, EEA or Switzerland and is transferred by Canary to Supplier for Processing in a country not subject to an adequacy decision in accordance with the GDPR ("**UK/EEA/Switzerland Data Transfer**"), the parties will conduct such UK/EEA/Switzerland Data Transfer in accordance with all applicable laws. The parties hereby agree to the Standard Contractual Clauses for EEA/Switzerland Data Transfers, together with the version as modified by the UK Information Commissioner's Office's international data transfer addendum ("**IDTA**") (together, "**EU SCCs**") (which will be deemed executed by the parties as of the effective date of the Agreement). For the purpose of this Section 5.2 the EU SCCs means Module Two (Transfer controller to processor) of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the text of which is available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en), and the IDTA means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses published by the UK Information Commissioner's Office (the text of which is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/) (or any successor IDTA approved by the relevant UK authorities) in which Canary will be referred to as the "data exporter" and Supplier will be referred to as the "data importer", incorporating: (a) the relevant Options set out in Part 1 of Attachment 2 to this DPA; (b) Annex I pre-populated with the details set out in Part 2 of Attachment 2 to this DPA; and (c) Annex II pre-populated with the details set out in Part 3 of Attachment 2 to this DPA. For the purposes of this Section 5.2, the EU SCCs will come into effect upon commencement of an EEA/Switzerland Data Transfer. If there is any conflict between the Sections of this DPA or the sections of the Agreement and the EU SCCs, in so far as the conflict relates to an EEA/Switzerland Data Transfer the EU SCCs will prevail.

6. SUBPROCESSORS.

1. Supplier may only authorize a third party or Subprocessor to process the Personal Information if:
    1. Canary provides prior written consent after Supplier supplies Canary with full details regarding such Subprocessor;
    2. Supplier enters into a written contract with the Subprocessor that contains terms substantially the same as those set out in this DPA and, upon Canary's written request, provides Canary with copies of such contracts;
    3. Supplier maintains control over all Personal Information it entrusts to the Subprocessor; and
    4. the Subprocessor's contract terminates automatically on termination of this DPA for any reason.
2. Supplier must list all approved Subprocessors in Attachment 1 and include any Subprocessor's name and location and contact information for the person responsible for privacy and data protection compliance.
3. Where the Subprocessor fails to fulfil its obligations under such written agreement, Supplier remains fully liable to Canary for the Subprocessor's performance of its agreement obligations. The parties consider Supplier to control any Personal Information controlled by or in the possession of its Subprocessors. Upon Canary's written request, Supplier will audit a Subprocessor's compliance with its obligations regarding Canary's Personal Information and provide Canary with the audit results.

7. COOPERATION; ASSISTANCE.
    1. **Data Subject's Rights Assistance**. Supplier shall fully cooperate with Canary to enable Canary (or its third party Controller) to respond to any requests, complaints or other communications from Data Subjects and regulatory or judicial bodies relating to the processing of Personal Information under the Agreement(s), including requests from a Data Subject seeking to exercise their rights under Data Protection Law. In the event that any such request, complaint, or communication is made directly to Supplier, Supplier must notify Canary immediately, and shall not respond to such communication without Canary's express authorization. Supplier will comply with any deletion instruction from Canary regarding Personal Information unless an exception under Data Protection Law permits it to retain Personal Information. If Supplier determines such an exception exists notwithstanding a deletion instruction from Canary, then Supplier will: (i) notify Canary of such exception; and (ii) defend and indemnify Canary for any claims arising from or related to Supplier's retention of such Personal Information.
    2. **Data Protection Impact Assessment Assistance**. Taking into account the nature of Processing and the information available to the Supplier, Supplier will assist Canary in ensuring compliance with the obligations under Articles 35 and 36 of the GDPR.

8. TERM AND TERMINATION. This DPA will remain in full force and effect so long as the Agreement remains in effect, or Supplier retains any Personal Information related to the Agreement in its possession or control (**Term**). Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Information will remain in full force and effect. Supplier's failure to comply with the terms of this DPA is a material breach of the Agreement. In such event, Canary may terminate the Agreement effective immediately upon written notice to Supplier without further liability or obligation.

9. LIABILITY AND INDEMNITY.
    1. **Liability**. Notwithstanding anything else to the contrary in the Agreement, Supplier agrees that:
        1. It shall be liable for any unauthorized use, exposure or loss of Personal Information (including Client Personal Data) arising under or in connection with the Agreement and the DPA to the extent such loss results from any failure of Supplier (or its Subprocessors) to comply with its obligations under the DPA and/or applicable law or regulation;
        2. any exclusion of damages or limitation of liability that may apply to limit Supplier's liability in

the Agreement shall not apply to Supplier's liability arising under or in connection with the DPA, howsoever caused, regardless of how such amounts or sanctions awarded are characterized and regardless of the theory of liability, which liability shall be expressly excluded from any agreed exclusion of damages or limitation of liability.

2. **Indemnity**. To the fullest extent permitted by applicable law, Supplier shall indemnify, defend, and hold Canary, including its Authorized Affiliates, and each of its affiliates, partners, principals, officers, directors, employees, subcontractors and agents harmless against any claims, suits, or proceedings and any resulting liabilities, fines, losses, damages, costs and expenses (including reasonable attorney's fees) that Canary may suffer or incur as a result of any act or omission on the part of Supplier or its subcontractors, or anyone acting on their behalf, that leads to Canary being liable for breach of Data Protection Law or a third-party contract.

10. RECORDS. Supplier will keep detailed, accurate and up-to-date written records regarding any processing of Personal Information it carries out for Canary, including but not limited to, the access, control and security of the Personal Information, approved Subprocessors and affiliates, the Processing purposes, categories of Processing, any transfers of Personal Information to a third country and related safeguards, and a general description of the technical and organizational security measures (**Records**). Supplier shall make this record available on request to Canary or any relevant EU or Member State supervisory authority. Supplier will ensure that the Records are sufficient to enable Canary to verify Supplier's compliance with its obligations under this DPA and Supplier will provide Canary with copies of the Records upon request.
11. AUDIT. Supplier shall, and shall procure that its agents and Subprocessors shall, make available to Canary, all information necessary and allow for and contribute to audits of such data processing facilities, procedures, records and documentation which relate to the Processing of the Personal Information, including without limitation, inspections (on reasonable written notice) by Canary, its auditors or agents or any regulatory or government body, including any supervisory authority, in order to ascertain compliance with the terms of this DPA or Data Protection Law.
12. SURVIVAL. Supplier's obligations under this DPA will survive termination of the Agreement and the completion of the Services.
13. CERTIFICATION. Supplier certifies that Supplier understands and will comply with the requirements and restrictions set forth in this DPA.
14. GENERAL
    1. **Governing Law**. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless and to the extent required otherwise by the Data Protection Law or, where applicable, the Standard Contractual Clauses.
    2. Parties acknowledge and agree that any breach by Supplier of the DPA shall constitute a material breach of the Agreement, in which event and without prejudice to any other right or remedy available to it, Canary may elect to immediately terminate the Agreement (in whole or in part) in accordance with the termination provisions in the Agreement
        1. **[SIGNATURE PAGE FOLLOWS]**

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed as of the date first written above by their respective officers thereunto duly authorized.

	Canary LLC.
	By_____ (Authorized Signature)

	Name: Title: Date:
	Supplier Full Legal Entity Name:
	By_____ (Authorized Signature) Name: Title: Date:

1. ATTACHMENT 1 Selected Options and Annex Details for the EU SCCs

Part 1 – Selected Options

Clause 7 (Docking clause)	Clause 7 will not be incorporated.
Clause 9 (Use of Subprocessors)	Option 2 and the specific time period referred to will be 14 days.
Clause 11 (Redress)	The Option in Clause 11(a) will not be incorporated.
Clause 13 (Supervision)	The following paragraph of Clause 13(a) will be incorporated: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
Clause 17 (Governing law)	Option 1 and the governing law will be the laws of Ireland.
Clause 18 (Choice of forum and jurisdiction)	The courts inserted will be the courts of Ireland.

Part 2 – Content of Annex 1 to the EU SCCs

A. LIST OF PARTIES

Data exporter:

Name:	Canary LLC dba Canary Marketing
Address:	2700 Camino Ramon, Suite 110, San Ramon, CA 94583 USA
Contact person's name, position and contact details:	Attn: Privacy e-mail: **privacy@canarymarketing.com**
Activities relevant to the data transferred under these Clauses:	The services as set out in the Agreement
Signature and date:	See signature page
Role (controller/processor):	Controller

Data importer(s):

Name:	
Address:	
Contact person's name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	The services as set out in the Agreement
Signature and date:	See signature page
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	**Categories of data subject**	**Please mark "X" for all that apply.**
	The Personal Information transferred concern the following categories of data subjects:	
	Canary Client Data: data subjects whose personal information is controlled by Canary's clients and for whom Canary is acting as a data processor.	☐
	Canary Workforce Data: past and present employees, directors and officers of Canary, including contractors or other beneficiaries and dependents of employees, or candidates for employment of Canary.	☐

	Canary Business Contacts: data subjects who have provided Canary with their Personal Information as part of business activities with Canary.		☐
Categories of personal data transferred:	**Categories of data**		**Please mark "X" for all that apply.**
	Contact details: name, title, email address, mailing address, telephone number, and other personal contact details.		☐
	Financial data: bank account number, bank details, credit card details or Cardholder Data.		☐
	Order data: purchasing history, return history, cancellation history.		☐
	Location data: approximate physical location information or specific geolocation.		☐
	Persistent Identifiers: device identifiers, Internet Protocol addresses; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, unique pseudonyms, user aliases, and any other persistent identifiers that can be used to recognize a consumer, a family, or a device that are linked to an individual or family, over time and across different services, or other forms of persistent or probabilistic identifiers that can be used to identify a particular individual or device.		☐
	Correspondence data: Correspondence and other communications (including lawfully recorded telephone communications data) with the data subject for the purpose of providing customer support.		☐
	Other categories of data (please describe further the type(s) of data that importer is receiving and for what purpose in the adjacent box).		
Sensitive data transferred (if applicable) and applied restrictions or safeguards:	**Sensitive data**	**Please mark "X" for all that apply.**	**If "X" is marked, explain the following for all categories that apply:** • **What sensitive data is involved** • **The extra restrictions or**

			safeguards to protect the data
	Special categories of data such as data related to children, genetic data, biometric data, health and disability data, data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs or government IDs(please describe further the type(s) of special data that importer is receiving and for what purpose in the adjacent box).	☐	
	None. N/A.	☐	
The frequency of the transfer	**Explain if the transfer is:**		**Please mark 'X' or type response in one of the following three boxes below**
	A once-off transfer		☐
	Happening on a continuous basis for the length of the Agreement		☐
	Another frequency (if applicable, give details)		
Nature and purposes of the transfer and processing:	The data importer will transfer and Process the Personal Information on Canary's instructions, for the purposes that are described in the Agreement between Canary and the data importer (eg. providing goods or shipping).		
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Supplier shall: (a) delete and securely erase all Personal Information (including any derivatives thereof) when Supplier no longer has a legitimate business need to retain them, but in no event longer than the earlier of (i) 30 days from the date Supplier receives the applicable Personal Information (unless otherwise expressly set forth by Canary), or (ii) 5 days after the termination or expiration of the Agreement.		
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	[If Supplier is using any Subprocessors, Supplier to also provide Subprocessor(s)': Name: Address: Contact Person's name, position, and contact details:		

	Description of processing:] [Otherwise, please list: None.]

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	• **For Personal Data protected under the EU GDPR:** Data Protection Commission, Ireland • **For Personal Data protected under the Swiss DPA:** Federal Data Protection and Information Commissioner (FDPIC) • **For Personal Data protected under the UK GDPR:** Information Commissioner's Office

Part 3 – Content of Annex II to the EU SCCs

As set out in Attachment 3.

ATTACHMENT 2 Security Measures

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 will:

1. 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;
2. promptly terminate an individual's access to Personal Information when such access is no longer required for performance under the Agreement;
3. maintain reasonable and up-to-date anti-malware, anti-spam, and similar controls on Supplier's networks, systems, and devices;
4. 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;
5. 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;
6. 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
7. 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:

1. Industry best standard encryption algorithm (e.g. AES-256, RSA, WPA-2);
2. Transport Layer Security "TLS" v1.2 or higher during transmission;
3. Full disk encryption of any laptops, smartphones, tablets, or other portable devices (collectively, "Portable Devices") using an encryption algorithm that meets or exceeds industry best practices; and
4. 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:

1. Consistently executed secure code reviews and testing either through manual peer review or via a code scanning solution;
2. 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;
3. Protection of test data and content and removal of test data and content before deployment to production;
4. System acceptance testing; and
5. 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:

1. enforce MFA for all administrative users of Supplier cloud services;
2. 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

3. 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 Subprocessor; 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.

- 1. **Endpoint Security Requirements**.
2. 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.
3. 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.
4. **Business Continuity and Disaster Recovery**.
5. Business Continuity Plan.
6. 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.
7. Disaster Recovery.
8. 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.

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. Notwithstanding this Section 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 Data Protection 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.