INFORMATION SECURITY ADDENDUM

A. Security of Data Processing

Provation has implemented and will maintain technical and organizational measures inclusive of administrative, technical, and physical safeguards to ensure a level of security appropriate to the risk of the data processing for the Subscription Services as described in this Information Security Addendum (the "Security Measures"). These Security Measures may be changed by Provation from time to time to take into account advancements in available security technologies and updated industry standard guidelines. However, Provation will not materially decrease the overall security of the Subscription Services (as defined in the Subscription Agreement).

This Information Security Addendum supplements the Master Service Agreement and all Orders (the "Subscription Agreement") existing between the Parties.

B. Provation Shared Responsibility Model

Provation Responsibilities

Provation is responsible for the confidentiality, integrity and availability of the Subscription Services and internal Provation information technology systems. The Security Measures include, but will not be limited to, the following measures for ensuring the ongoing confidentiality, integrity, and availability of Customer Content (as defined in the Subscription Agreement) to prevent unauthorized access, use, modification, or disclosure of Customer Content:

a) performance of background checks on all personnel, as well as signature of non-disclosure commitments and business ethics prior to employment;

b) security and privacy awareness training, inclusive of acknowledgment and agreement to abide by organizational security policies, for all personnel upon hire and annually thereafter; this training includes secure development training for appropriate personnel;

c) Secure transmission of Customer Content in transit and at rest utilizing industry-standard encryption mechanisms for the Subscription Services;

d) the ability to restore the availability and access to Customer Content in a timely manner in the event of an incident impacting the availability of Customer Content by maintaining a geo-redundant backup solution for disaster recovery purposes;

e) logging and monitoring of security logs via a Security Incident Event Management ("SIEM") system and alerting to a dedicated Incident Response team upon the detection of suspicious system and/or user behaviors;

f) processes and tooling for regularly identifying, assessing, triaging, and remediating vulnerabilities based on industry-standard guidelines;

g) maintenance of a comprehensive and industry standard set of security and privacy policies, procedures and plans that are reviewed on at least an annual basis and provide guidance to the organization regarding security and privacy practices;

h) processes for evaluating prospective and existing Third Party Providers (as defined in the Subscription Agreement) to ensure that they have the ability and commit to appropriate technical and organizational measures to ensure the ongoing confidentiality, integrity, and availability of Customer Content;

i) process for regularly testing, assessing, and evaluating the effectiveness of administrative, technical, and physical safeguards for ensuring the security of the processing, transmission, or storage of Customer Content through external and internal audits as further described in Section C below;

j) monitoring the environment for suspicious activity designed or intended to impair the operation of any computer or database or prevent or hinder access to, or the operation of, any program or data, using detection software generally accepted in the industry;

k) securing computing environments according to generally accepted industry standards to ensure no access by any unauthorized person or malicious software, and implementing the principal of least privilege to minimize unnecessary access;

l) preventing access, use, modification, or disclosure of Customer Content except by authorized Provation personnel (1) to provide the Subscription Services and prevent or address service or technical problems, (2) as compelled by law, or (3) as Customer expressly permits in writing;

m) notifies Customer of a security breach of which it becomes aware and appropriate remediation;

n) Multi-Factor Authentication ("MFA") for all personnel with administrative and/or remote access;

o) conduct regular review of user accounts to identify, remove, or disable accounts;

p) denial of offshore access to Customer Content from outside the United States;

q) restricting access, export or storage of Customer Content outside the United States without Customer's prior written consent;

r) maintenance of an inventory of all computers, servers, applications, and information systems;

s) employment of i) technical and non-technical safeguards to restrict the use of removable media and portable storage devices which limits the use of portable storage devices to only Provation issued devices; and ii) sanitization of information system media prior to disposal, release from organizational control, or release for reuse in accordance with organizational policies;

t) employment of, but not limited to, server-level patching, vulnerability management, network segmentation, code scanning, penetration testing, security event logging & monitoring, incident management, operational monitoring, 24/7 support, and ensuring Customer availability in accordance with the applicable SLA.

In addition to the above, Provation also maintains the two following programs:

(1) A System Development Lifecycle ("SDLC") and change management program that aligns with the ISO27001 framework and Provation's corresponding ISO27001 certification. As part of the Provation software development process, internal testing and Quality Assurance is completed for each software update prior to production deployment.

(2) Third-Party Risk Management (TPRM) program that requires Third Party Providers to maintain strong security measures and mandates an assessment before onboarding. Provation conducts due diligence to assess and manage Third Party Provider risk, ensuring Third Party Providers implement security controls to protect against threats, limit harm from potential adversaries targeting the organizational supply chain, and avoid introducing unnecessary risks. Additionally, Provation's Third Party Business Integrity Program ensures Provation only partners with Third Party Providers committed to ethical and transparent business practices.

By implementing the Security Measures and programs detailed above, Provation considers the risks related to data processing, in particular the risks resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

Customer Responsibilities

The Customer is responsible for their applications' security, including managing users who may utilize a Provation account, Customer access management, password rotation and reset, multifactor authentication, as well as any other security measures required by their organization. In addition, the Customer is also responsible for (a) the secure management of their users that they manage and provision for the purpose of granting access to the Subscription Services, (b) complying with the terms of the Subscription Agreement, and (c) complying with Provation's Acceptable Use Policy.

C. Third Party Audits, Certifications

The Subscription Service Security Measures are subject to periodic testing by independent third-party audit organizations, inclusive of the following audits and certifications and attestations:

- SOC 2 Type II
- ISO 27001
- ISO 27701
- ISO 22301 (Provation Apex only)
- ISO 27017
- ISO 27018
- HIPAA Type I

Upon written request, Provation will attest to such independent third-party audits or provide copies of its current SOC2 Type II audit report for the Subscription Services to Customers following execution by Customer of Provation's Security NDA. The Subscription Services use Microsoft Azure and a one-to-many business model that relies on standardization of best practices and industry standards for the benefit of its Customers. Onsite audits by Customers pose security and privacy risks to Provation, other Provation Customers, and Third Party Providers. Moreover, Microsoft Azure does not allow for physical audits of its data centers but instead provides evidence of its security via https://www.microsoft.com/en-us/trust-center/product-overview/. Therefore, Provation's security program consists of third-party audits, certifications, and available documentation detailed in "Third Party Audits, Certifications," and does not allow audits by Customers or third parties, except for those it selects to obtain the listed certifications.