BEACON PLATFORM INCORPORATED
INFORMATION SECURITY POLICY

1. **Security Safeguards**. Beacon Platform Incorporated (“**BPI”)** maintains and complies on behalf of its clients (each a “**Client**”) with an appropriate and comprehensive information security program, including policies and procedures, to ensure the confidentiality, security, integrity, and availability of our client’s data (“**Client Data**”) and the software and associated user interfaces and related technology that Beacon makes available to its clients (the “**Platform**”) and that includes administrative, technical, and physical safeguards (including reasonable disposal to safeguard Client Data and the Platform against unauthorized access, use, disclosure, modification, unavailability and deletion). BPI operates and maintains such safeguards in accordance with the requirements of its agreements with its clients, all applicable law and regulations and good practices. All confidential information supplied by a party to the other party shall remain solely and exclusively the property of the disclosing party. Without limiting the foregoing, such safeguards are implemented and maintained by BPI as follows:

(i) no less than once annually, mandatory security awareness training for all BPI personnel (including management and consultants), which includes (A) training on how to implement and comply with its information security program; and (B) promoting a culture of security awareness through periodic communications from BPI senior management to BPI personnel;

(ii) use of up-to-date cybersecurity technologies and practices, including appropriate network perimeter, multi-factor authentication, and other access controls and monitoring, as well as encryption of Client Data in accordance with Traffic Encryption Within Beacon Platform;

(iii) physical security procedures, including security guards, and camera surveillance and electronic logging of facilities access (e.g., key cards) systems, in each case, at entry points to critical work areas at BPI office locations (data center security is the responsibility of the relevant cloud provider);

(iv) to the extent permitted by applicable law, background checks on employees, consultants, and other personnel with access to Client Data or the Platform, and require that our suppliers with access to Client Data or the Platform perform background checks on their personnel that are no less comprehensive than the background checks performed by BPI;

(v) restriction on access to and use and copying of Client Data on a “need-to-know” basis;

(vi) regular monitoring of the transport and storage of Client Data and the associated Platform is performed by the relevant cloud provider;

(vii) regular penetration testing and vulnerability assessments of the Platform, prompt remediation of any found deficiencies and prompt notification to Client with detail to allow a Client to take action, if any, to mitigate any adverse impact on a Client or Client’s systems, and BPI provides Clients with a summary of the penetration test reports upon request;

(viii) due diligence and regular monitoring (including relating to financial and operational stability, reputation, security, and technical abilities) of BPI personnel with access to the Platform and/or facilities or working on a Client's systems and/or facilities;

(ix) logical segregation of Client Data from other information and/or data accessed, stored, or hosted by BPI (or any of its subcontractors or other third party);

(x) ethical walls and internal procedures when providing services to a Client or any third party to prevent breaches of confidentiality;

(xi) security measures to manage (including the means to remotely wipe) BPI issued mobile devices; and

(xii) promptly upon termination of employment or engagement, as applicable, of BPI personnel with access to the Platform, Client Data, and/or Client's systems, disabling all such access and (if applicable) notifying Client to disable any Client-controlled access methods or permissions with respect to such terminated BPI personnel.

2. **Information Provision**. Upon request, BPI will promptly provide a Client with its SOC 2 Type 2 Report.

3. **Client Data Locations**. Client Data will be stored either (a) on a Client's instance with its cloud provider, or (b) within a single-tenant client segregated account hosted by BPI (in which case BPI will inform a Client as to the location of such Platform instance).

4. **Use of Client Data and Client Systems**. BPI uses Client Data and a Client's systems only as necessary to provide the Platform and the Services in accordance with its agreements with its clients. As agreed between a Client and BPI, Client retains all right, title, and interest in and to all Client Data and a Client's systems.

5. **Breach Notification and Remediation Requirements**.

   (a) If BPI learns or has reason to believe that: (i) there has been unauthorized access, use, modification, or deletion of Client Data, or (ii) there has been unauthorized access or use of a Client's systems or the Platform (each, a "**Cybersecurity Event**"), BPI will immediately and in no event more than twenty-four (24) hours from becoming aware of such Cybersecurity Event, provide notice of the Cybersecurity Event to a Client. Such notice must be sent to an email address approved in writing by a Client and must include all material details of the Cybersecurity Event, which material details BPI shall retain per BPI's then current retention policy.

   (b) BPI will: (i) promptly use commercially reasonable efforts to contain, control, and remediate any Cybersecurity Event to prevent future unauthorized access to or misuse of Client Data, Client Systems, or the Platform; and (ii) provide updates to a Client, upon request, relating to the investigation and resolution of the Cybersecurity Event.

6. **Disposition and Portability of Client Data**. For BPI hosted Platform instances, a Client shall have six (6) months following termination of its agreement with BPI, the ability to download a copy or

all copies of Client Data from the Platform. Promptly thereafter, BPI shall instruct the relevant cloud provider to delete the Platform instance and all Client Data within. Upon request by a Client, an officer of BPI will promptly certify in writing to the Client that BPI has given such instruction.

7. **Inspections**. BPI provides to a Client's regulators or other law enforcement agents access at all reasonable times to any facility (or part of a facility) controlled by BPI and to data and records relating to the Services and the Platform and/or a Cybersecurity Event for the purpose of performing audits designed to enable a Client's regulators or other law enforcement agents to confirm that BPI is meeting all applicable information privacy and security requirements, and regulatory and other legal requirements.

   When BPI uses any cloud provider (such as Amazon, Google, or Azure) (each a "Cloud Provider" and, collectively, the "**Cloud Providers**") to provide the Platform instance, then BPI will, upon request by such Client's regulator or other law enforcement agent, promptly demonstrate to such Client's regulator or other law enforcement agents that such Cloud Provider's security configurations and controls (including policies and procedures) meet all applicable information privacy and security requirements, and regulatory and other legal requirements. In the event Client's regulator or other law enforcement agent notifies BPI of any deficiencies or noncompliance identified in this Section 2.7, BPI will review such notification and will advise Client's regulators or other law enforcement agents of any and all steps taken to remediate such deficiencies and/or noncompliance.

8. **Attestations and Reports**.

   (a) At least once annually, at BPI's expense, BPI retains a reputable external auditor to complete their respective: Service Organization Controls 1 & 2, Type 2 Reports ("**SOC Reports**") (or, in each case, substantially equivalent successor standards issued by the relevant governing body, or if none, a comparably detailed audit). BPI maintains a data processing environment and internal controls that provide at least the same level of protection as evidenced by the controls described in BPI's then-current SOC Reports. If Client reasonably believes, and BPI agrees, that the SOC 2 Type 2 Report does not address any requirements set out in the Agreement, BPI will include the missing requirements in the next such report.

   (b) BPI employs and maintains a cybersecurity program under the supervision of information security and compliance departments headed by personnel with sufficient experience and authority who utilize reasonable commercial practices for information security management.