Revised 06-10-2020

Propel, Inc., Information Security Management Policy (ISMP)

1.0 PURPOSE/OVERRIDING SECURITY OBJECTIVE/POLICY REVISION AS "BIG PICTURE" REVIEW OF PROPEL PLATFORM: The purpose of Propel's ("Propel" or "Company") ISMP is to establish and maintain a set of evolving security controls (working compliance policies) for its information system. In the broadest possible terms, Propel's information system is an integrated set of components used to manage, collect, store and process personal data (PD). These components include hardware and software applications, database(s), network(s) and the people involved therewith. The defense of these systems must necessarily encompass management and oversight of both the infrastructure and any relevant path, by which any number of risks or threats (which come in all shapes and sizes, as well as from varying sources) can gain access to, and meaningfully disrupt the operation of the Propel® platform. Our overriding security objective is to secure and keep private, the protected information that the Company handles in conjunction with its clients, its clients' employees, its third-party data center host and other mission related third-party vendors, etc. In short, data security for the purpose of maintaining privacy is vitally important. Finally, as a practical matter, each Propel policy, information security sub-policy, protocol or defined process ("policy" or "sub-policy") represents an integral part of Propel's ISMP (see **Section 12.0 below** for a policy listing). Because each policy is critical to the desired synergy, any policy revision (performed with a "big picture" approach), constitutes an exercise in risk management, which in turn, becomes the basis upon which the Company can assert that each such revision constitutes a meaningful part of the Company's ongoing Data Privacy Impact Assessment (DPIA). This means that because of the factors considered with any policy revision (see **Section 8.0 below**), Propel has in fact conducted an ongoing risk assessment of its platform and performed an updated DPIA.

2.0 SCOPE: This ISMP applies to all team members, contractors, vendors and agents (hereinafter referred to as "Authorized Users") with access privileges to Propel's network. The policy's rules also apply to sending E-Mail and viewing intranet/internet web resources.

3.0 PROPEL OVERVIEW AND BUSINESS DESCRIPTION: Propel, Inc., is engaged in the development, maintenance and support of the Propel® platform. More specifically, Propel is a Software as a Service (SaaS) platform, designed to run and manage comprehensive wellbeing programs.

4.0 OPERATIONAL SECURITY (OPSEC) CONSIDERATIONS: The title of this policy is informative; it implies the need for discretion, for keeping many details confidential. Thus, designed for a balanced approach, every effort is made to explain the Company's information security management efforts, without identifying specific item nomenclature, vendor relationships or technology baselines. However, any client, third-party or vendor collaborating with Propel and/or its client relationships is welcome to request more specific information at (privacy@propelwellness.com).

5.0 UNDERSTANDING THE PROPEL PLATFORM / CLIENT DATA BACK-UP AND RECOVERY/DYNAMICS OF THE THIRD-PARTY DATA CENTER ENVIRONMENT: Crucial to this ISMP, is the concept of how Propel's clients can access and utilize their data. Each client has a separately installed web application and database (accessed through a client portal), which is located on one of the servers managed by Propel, but physically maintained for Propel by its third-party data center host at multiple data center locations. Daily backups of all databases for the Propel® platform servers (including those used as client portals) are conducted in accordance with configuration instructions furnished by Propel when servers are brought

online. Further, client back-up data is stored in multiple data center facilities within a single geographic region. These servers are physically maintained, protected, guarded and carefully hosted within the data center environment pursuant to written agreement between Propel and its third-party data center host. Specifically, these client portals use dedicated "bare metal servers" maintained solely for Propel and its clients. In simple terms, this means that such servers are not cloud based and are not shared. In addition, the use of such dedicated bare metal servers has two important operational advantages. First, any risk of improper or deficient load sharing is mitigated, the existence of which could affect the ability of our clients to access their respective data in a crisis. Second, more than 99% of our clients' employees' PD is handled within the confines of the carefully controlled data center environment, and NOT on Propel's corporate/office server. Each data center is designed with a focus upon redundancy in its infrastructure systems and Network Point of Presence (POP). This POP technology (housed in the data center's carefully controlled environment) enables Propel's U.S.-based clients and non-U.S.-based clients to have a safe and secure access point from the data center to the rest of the internet. The Propel platform also includes one virtual "staging" server (machine) in the data center, dedicated to staging and testing as client portals are made ready for initial launch, or to provide a secure stage upon which the entire range of testing (from interim to final) can take place in support of the Company's system development life cycle (SDLC) or change management processes. Two of Propel's Information Security Sub-Policies describe and control these processes (*Propel, Inc., Information Security Sub-Policy Number 3—Platform System Development Life Cycle (SDLC) Compliance; and Propel, Inc., Information Security Sub-Policy Number 7—Change Control Management)*.

6.0 THE COMPANY'S INFORMATION SECURITY RESPONSIBILITIES IN SUPPORT OF THE PROPEL® PLATFORM/NECESSARY SUB-POLICIES: Propel's primary information security responsibilities are centered around its operational, software and coding support of the Propel® Platform. Simply stated, prior to the commencement of actions needed to "stand-up" a client's website program portal on the Propel® platform, necessary infrastructure work is performed by Propel's Information Technology (IT) team members regarding the development, design, production and maintenance of pre-customized wellbeing plans (without any PD). This work is performed on the Company's corporate/office server. Once the "website stand-up" process begins, all work associated therewith, is performed on the Propel platform server(s). Titled as Information Security Sub-Policies, etc., each establishes guidelines and standards for team members to get specific jobs done in an ethical fashion and ever mindful of the Company's overriding data security objective, to secure and keep private, our program participants' PD. These sub-policies, etc., are listed below in **Section 12.0** below.

7.0 THE REGULATORY ENVIRONMENT (APPLICABLE LAWS, REGULATIONS AND DIRECTIVES): Propel pays special attention to HIPAA related security and privacy requirements, as well as the requirements of the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the Personal Information Protection and Electronic Documents Act (PIPEDA). Additionally, it is important to note that the Company strives to comply with both the letter and spirit of such laws. When appropriate, compliance policy details are drawn in such a way that Propel strives to meet or exceed even the most strenuous of applicable laws and regulations, which precludes the necessity of drafting separate compliance policies.

8.0 POLICY REVISION AS CONTINUING EXERCISE IN RISK MANAGEMENT / DATA PRIVACY IMPACT ASSESSMENT (DPIA): As stated in **Section 1.0 above**, the process of revision for each compliance policy, etc., also constitutes a "big picture" review of the Propel platform and represents an exercise in continuing

risk management. This is because each policy revision contains a review/consideration of at least the following items:

- the Company's responsibilities relating to PD;
- that each client develops its own privacy notices and policies for posting on its wellness program portal (after reviewing Propel's proposed Terms of Use Policy and Consent Agreement which in effect constitutes a portal specific privacy policy);
- that all PD processed by Propel is authorized via a transparent, clearly stated, "opt in" consent process;
- that Propel does not sell or otherwise share PD with any third-party (outside the requirements of the wellness program), without the consent of its client's program participant(s), except as may be required by law;
- that a review of Propel's information, data and cyber security programs then in effect, reveal no unusual vulnerabilities;
- that a review of Propel's application development security posture reveals no unusual vulnerabilities. This effort represents an effort to determine if a reasonably foreseeable system flaw or weakness in an application, would likely be exploited by an attacker. Thus, the question becomes, "once identified, would an attacker likely use the flaw or weakness as a path along which any number of malware threats, etc., might reasonably be expected to travel, in order to gain access to, and meaningfully disrupt the operation of the Propel® platform?"
- that all PD is encrypted at rest, in transit and in storage;
- that the Company's use of encryption technologies is quite extensive and continually updated;
- that a review of all information security sub-policies and privacy policies, etc., (see **Section 12.0 below**) reveals no additional vulnerabilities;
- that there is no history of PD breach or compromise;
- that the Company's Data Protection Officer (DPO) has reviewed (for regulatory updates) at a minimum the websites of the following organizations, whose owners have information and/or enforcement authority of privacy laws in their respective jurisdictions: a) The Information Commissioner's Office in the United Kingdom, b) Office of the Privacy Commissioner of Canada, c) U.S. Department of Health & Human Services, and d) State of California Office of the Attorney General;
- that Propel's President & Chief Executive Officer (CEO) approves all non-housekeeping policy revisions; comments, suggestions, etc., are always welcome from the Chief Administrative Officer (CAO) and Vice President-Application Architecture (VP-AA); and finally, each DPIA (if memorialized in writing) ends with the following language (if appropriate): "from all of which the DPO finds that pursuant to requirements and guidance of GDPR, CCPA, and others, there is no need to conduct a more formalized DPIA at this time, that the risk/potential for harm is extremely low, as is the likelihood and severity of impact upon client's employees/program participants.

9.0 THIRD-PARTY DATA CENTER CERTIFICATIONS ARE VERY IMPORTANT: Each of Propel's third-party hosted data centers is designed with a focus upon redundancy in its infrastructure systems. Propel contractually relies upon the expertise and security certification(s) maintained by its third-party data

center host, to secure and keep private the protected data which it handles, stores and preserves for back-up. In short, Propel relies upon its third-party data center host to deliver upon its promise to meet strict industry guidelines as evidenced by its possession of numerous compliance certifications, etc. The compliance evidenced by these certifications is at the heart of Propel's decision making process to select its third-party data center host. See Section 5.0 of *Propel, Inc., Information Security Sub-Policy Number 1—Privacy, GDPR and CCPA Compliance and* Section 5.0 of the *Propel Third-Party Due Diligence and Risk Management Policy*.

10.0 ROLES AND RESPONSIBILITIES/PROPEL'S INFORMATION SECURITY MANAGEMENT COMMITTEE: Development, steering and oversight of Propel's ISMP is vested in an Information Security Management Committee, presently consisting of three (3) members and serving at the pleasure of the President and Chief Executive Officer (CEO). Sitting as Co-Chairpersons of the Committee are the CAO and the VP-AA. Serving as the Committee's Secretary is the Chief Compliance Officer (CCO) who is also charged with taking minutes of formal meetings and drafting the various compliance policies. Further, in an effort to comply with the letter and spirit of applicable laws, (GDPR, CCPA, PIPEIDA and LGPD (the Brazilian General Data Protection Law), Propel, Inc., designates its CCO to assume the additional responsibility as DPO. The committee meets periodically (oftentimes informally as a working group) as may be necessary and any of its members can call for a formal meeting of the Committee. Generally, the Committee is empowered to provide information security guidance to the Company, establish security standards and guides for protecting information/data assets, deliver guidance regarding needed information security policies, periodically review security risks/threats and offer suggestions to the CEO regarding matters relating to information technology. Finally, the Committee shall act as the Company's investigative arm for resolution, reporting and tracking of information security issues. The CEO shall serve as the sole appellate authority regarding all Committee matters, and in his sole discretion override or preempt actions of the Committee.

11.0 POLICY COMPLIANCE

11.1 Compliance Measurement: Propel's CCO, in consultation with the Information Security Management Committee will verify compliance to this policy through various methods, which may include, but not be limited to one or more of the following: periodic internal and external technology audits, walk-throughs, video monitoring, business tool reports, inspection and log review. Feedback will be provided to the CAO, Information Security Management Committee and appropriate business unit manager(s).

11.2 Exceptions: Any exception to the policy must be approved in advance by Propel's CAO and the Information Security Management Committee.

11.3 Non-Compliance: A team member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment for even the first offense.

12.0 RELATED STANDARDS, POLICIES AND PROCESSES

Please review the following related policies for details about protecting both Company and client information using this policy:

- *Propel Code of Conduct/Business Ethics Policy*
- *Propel Third-Party Due Diligence and Risk Management Policy*

- *Propel Business Continuity Plan (BCP)—Disaster Recovery Plan (DRP)*
- *Propel Information Security Sub-Policy Number 1—Privacy, GDPR and CCPA Compliance*
- *Propel Information Security Sub-Policy Number 2—Electronic/Physical Media Sanitation, Disposal and Transfer Compliance*
- *Propel Information Security Sub-Policy Number 3—Platform System Development Life Cycle (SDLC) Compliance*
- *Propel Information Security Sub-Policy Number 4—Password Protection-User Responsibility Compliance*
- *Propel Information Security Sub-Policy Number 5—Acceptable Encryption; Technologies in Use*
- *Propel Information Security Sub-Policy Number 6—Visitor Access and Control*
- *Propel Information Security Sub-Policy Number 7—Change Control Management*
- *Propel Information Security Sub-Policy Number 8—Platform Application Development Security*
- *Propel Information Security Sub-Policy Number 9—Intrusion Prevention and Platform Security Incident Response Procedures*
- *Propel Information Security Sub-Policy Number 10—Encryption Key Management*
- *Propel Information Security Sub-Policy Number 11—Vulnerability Management and Penetration Testing*
- *Propel Information Security Sub-Policy Number 12—Information Technology (IT) Asset Management (ITAM) and Patch Management*
- *Propel Information Security Sub-Policy Number 13—Cyber Security*
- *Propel Remote Technology Access Policy*
- *Propel Acceptable Use Policy*
- *Propel Platform Problem Management Policy and Procedures*
- *Propel Records Management, Document Retention and Disposal Policy*
- *Propel HIPAA Workstation Security Policy*
- *HIPAA Security Rule Requirements-Physical Safeguards Policy*
- *HIPAA Security Rule Requirements-Administrative Safeguards Policy*
- *HIPAA Security Rule Requirements-Technical Safeguards Policy*
- *HIPAA Protected Health Information (PHI) Use and Disclosure Policy*
- *HIPAA Privacy Policy, The Complaint Process and Breach Notification.*

Revision History: Date	Revision No.	Description of Changes
07-25-2018	01	Establish a more formalized Information Security Management Policy (ISMP), as well as to distinguish information security (IS) efforts for our third-party data center relationship from those relating to our Intra-Company server.
09-05-2018	02	Update Business Overview Section 3.0
11-28-2018	03	Substitute VP-AA for VP-IT on the Information Security Management Committee.
02-22-2019	04	Standardize some wording to conform to other policies…no formal approval needed for these housekeeping changes.

10-31-2019	05	Continue to standardize wording to conform to other policies; add compliance to CCPA; more explanatory changes to Section 6.0.
06-10-2020	06	Make material revisions to the ISMP; conduct Data Privacy Impact Assessment (DPIA); formalize the process which ensures that with every policy revision, an updated DPIA is conducted which ensures continuous risk management oversight and "big picture" review of the Propel platform.