Revised 02-22-2019

Propel, Inc., Information Security Sub-Policy Number 5—Acceptable Encryption; Technologies in Use

1.0 AUTHORITY/PURPOSE/OBJECTIVE: *Section 6.0 of the Propel, Inc., ("Propel" or "Company") Information Security Management Policy ("ISMP")* incorporated herein by reference and available upon request, identifies the need for sub-policies to address a variety of information security subjects, two of which are to establish guidelines for choosing acceptable encryption technologies and to identify those technologies currently in use by the Company. If deployed correctly, encryption can serve to achieve flexibility and an improved compliance posture, which in turn supports the absolute need for data privacy. This sub-policy is used to help secure and keep private the protected data (PD) 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.

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

3.0 BACKGROUND/HIPAA and HITECH/POLICY: HIPAA and HITECH require organizations that fall within the definition of a "Covered Entity" to provide clear policies to address the protection of specified health information. This sub-policy describes the encryption safeguards employed by Propel® to secure Protected Health Information (PHI) as such information is collected and stored on behalf of clients that have contracted with the Company to use the Propel® platform. Under HIPAA and HITECH each of Propel's clients is known as a "Covered Entity." Propel, Inc., is considered a "Business Associate" of a Covered Entity. As a Business Associate, it is critically important to have structured and appropriate controls that address access to potential PHI of a Covered Entity's employees. Such access controls enable authorized users to access only the minimum necessary information needed to perform job functions. Specifically, HIPAA requires the implementation of technical policies and procedures for electronic information systems that maintain electronic PHI, and to allow access only to those persons or software programs that have been granted appropriate access rights.

4.0 ACCEPTABLE ENCRYPTION: The use of encryption technologies is limited to those algorithms which have received substantial public review and have been proven to work effectively. Propel acknowledges and embraces the following limitations: a) proprietary encryption algorithms are not allowed for any purpose unless reviewed by a qualified expert other than the vendor in question and approved by the Information Security Management Committee; b) the use of "MD5," "Dual Eliptic Curve" and "Extended Random" algorithms are likewise not allowed for any purpose unless reviewed by a qualified expert other than the vendor in question and approved by the Information Security Management Committee; and c) export of encryption technologies may require a permit from the Department of Commerce (Bureau of Industry and Security-BIS) and as such, consultation with BIS is necessary prior to export**.**

5.0 ENCRYPTION TECHNOLOGIES IN USE/SPECIFICS: Among the technical safeguards employed by Propel are sophisticated data encryption processes to secure the data. Specifically, these encryption

processes can be summarily described as follows: Full drive/disk encryption is utilized and as such data at rest is encrypted. Data back-ups "at rest or in use" are stored using Advanced Encryption Standard (AES) 256-bit encryption. Data back-ups "in transit" are encrypted over the wire (OTW) using AES 256-bit-encryption. Further, all data in transit/motion is encrypted using Transport Layer Security (TLS) technology; its predecessor, Secure Sockets Layer (SSL) has been expressly disapproved by the Internet Engineering Task Force (IETF). TLS is a cryptographic protocol which provides communications security over a computer network and addresses both data integrity and privacy concerns between two or more communicating computer applications. File feeds such as the receipt of client eligibility files, biometric screenings and activity files are protected by Pretty Good Privacy ("PGP" and named for PGP Corporation, founded in 2002 and acquired by Symantec in 2010) encryption software.

6.0 BACKGROUND/GDPR/POLICY: While the GDPR does not specifically mandate the use of encryption technology, it does require businesses to implement "appropriate technical and organizational protection measures" to provide appropriate protection to the personal data (PD) held by them. Under the GDPR such measures now include encryption of PD. What is important for purposes of this sub-policy is the fact that Propel does in fact employ encryption technology as described in Section 5.0 above. This use of such technology, together with and in reliance upon the compliance credentials and certifications of IBM Cloud, serve to demonstrate Propel's commitment to comply with both the letter and spirit of applicable laws.

7.0 POLICY COMPLIANCE

7.1 Compliance Measurement: Propel's Chief Compliance Officer (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).

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

7.3 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.

8.0 RELATED STANDARDS, POLICIES AND PROCESSES

Please review the following policies for details of protecting information when assessing and using encryption technologies:

- *Propel Information Security Management Policy (ISMP)*
- *Propel Information Security Sub-Policy Number 10--Encryption Key Management Policy*

Revision History: Date	Revision No.	Description of Changes
08-14-2018	01	Establish a broader encryption policy that references both HIPAA and GDPR as well as to bring Propel's technology applications up-to-date.
10-25-2018	02	Enlarge the sub-policy to include "acceptable encryption technologies" and selection guidelines and limitations…enlarge name of sub-policy to Acceptable Encryption; Technologies in Use.
02-22-2019	03	Standardize policy language to conform to other policies…no formal approval required for these changes.