Revised 02-22-2019

Propel, Inc., Information Security Sub-Policy Number 3-Platform System Development Life Cycle (SDLC) Compliance

1.0 AUTHORITY/PURPOSE/OBJECTIVE/INFORMATION SECURITY ASPECTS: 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, one of which is a general set of procedures to govern the Propel® platform System Development Life Cycle (SDLC) process. These procedures are placed into sub-policy format to stress their importance in the Company's ongoing effort to ensure secure, streamlined, efficient and cost-effective governance, development and maintenance of the Company's Propel® platform. It is important to understand that the dynamics of this SDLC process have evolved over the years. The Company has adopted this platform style based on extensive platform development and management experience. The Company's staffing decisions are influenced in part by the level of support required for this platform style. The stated objectives of this sub-policy are to describe the stages which make up the SDLC for compliance purposes, integrate security oversight into the decision-making processes for each stage, as well as to invite continuing review, questions, comments and suggestions by team members.

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 POLICY/SDLC TYPE/STAGES/SECURITY OVERSIGHT TO ASSIST QUALITY ASSURANCE (QA): Web applications or components of a web application are all subject to the same design and development stages using the SDLC. Propel employs an "agile software development life cycle" which means that it is based upon the iterative and incremental design model, one that calculates a desired result by means of a repeated cycle of operation, refinement, and testing. It focuses upon the collaborative effort of the Company's cross-functional teams with those of our clients. It is characterized by quick delivery of work product, continual improvement and rapid response to changing circumstances. The stages in the Propel SDLC include the following: Concept, Iteration(s), Construction, Release, Production and Retirement. Each is considered in more detail below. Further, because of the security considerations that surround Propel's core source code (written and continually refined through each stage of the cycle), the Company includes one or more member(s) of the Information Security Management Committee into the decision-making processes occurring during each stage of the development life cycle. This is especially important during the "Concept" and "Release" stages of the cycle. A collateral benefit of this security integration is that it serves to enhance the Company's quality assurance (QA) effort, which in turn serves to ensure that the application(s) being deployed are secure upon release without creating delay that may result from deferring any security review until the end of the process.

4.0 CONCEPT: The concept phase of the SDLC utilized by Propel involves full project scope and overview. The stakeholders, whether that be Propel team members or a Propel client, will meet with Propel business analysts and project managers to fully outline and define the scope of the new development request. This project concept document is then broken into multiple components. Each component consists of features dependent on the others or which contain integrated functionality that result in a self-contained module. This means that once the component is developed, it can be tested on its own. The business rules for each component are documented and the process is flowcharted, indicating where the component falls in the overall project scope. The components are often placed in a priority or functionality order in preparation for the next stage.

5.0 ITERATION(S): Iterations occur after the Concept phase is completed. Each iteration consists of the selection by the development team and project manager of a component to be developed. The business rules and accompanying specifications for the component are reviewed and a timeline set for development. The iteration will begin with a meeting of the developers assigned to the selected component development, review of the timeline and weekly meeting day and time established for the specified iteration timeline. Multiple iterations can occur concurrently based on team availability.

6.0 CONSTRUCTION: Construction begins on the selected component and weekly meetings result in updates to the component specifications/notes to be reviewed by others on the team.

7.0 RELEASE: Release involves releasing the completed component code to the staging server to be tested by the internal Quality Assurance (QA) team, reviewed by the stakeholders, and notes, bugs, or other information gained during this stage added to the specification documents for the component. Should it be determined that the component iteration needs to return for additional development, the component will return to the Construction stage and upon completion be released to staging again following the same steps.

8.0 PRODUCTION: Production involves moving the completed project from staging to production. There are some components that can be moved into production individually while other components must stay in the release phase until all related components have been completed so that a more functional and complete version of the project can be moved into the production environment for general use.

9.0 RETIREMENT: Retirement occurs with the project once all the components defined in the initial Concept document have been released and moved into production.

10.0 POLICY COMPLIANCE

10.1 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).

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

10.3 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.

11.0 RELATED STANDARDS, POLICIES AND PROCESSES

Please review the following related policy for details about protecting both Company and Client information using this sub-policy:

- *Propel Information Security Management Policy*

Revision History: Date	**Revision No.**	**Description of Changes**
12-17-2017	01	Establish a more formalized System Development Life Cycle (SDLC) Document to frame the Propel® Platform project management process.
08-09-2018	02	This update indicates that the policy has been reviewed and integrates security oversight into the life cycle process.
02-22-2019	03	Standardize policy language to conform to other policies…no formal approval required for these changes.