Revised 02-23-2019

Propel, Inc., Information Security Sub-Policy Number 7—Change Control Management

1.0 AUTHORITY/PURPOSE: 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 set of standard operating procedures (SOPs) to manage the change control process. This Propel® Information Security Sub-Policy seeks to demonstrate that the Company continually strives to meet or exceed regulatory compliance expectations which arise from the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the more recently enacted European Union (EU) legislation known as the General Data Protection Regulation (GDPR). These procedures are placed into policy format to stress their importance in the Company's ongoing effort 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, International Business Machines (IBM) Cloud and other mission related third-party vendors, etc.

2.0 OBJECTIVE(S): This sub-policy seeks to manage and implement an appropriate set of standard operating procedures (SOPs) into the activities which surround a need or perceived need for making changes to critical, company information resources. Such resources include hardware, software, system documentation, operating procedure or some other information system application. These SOPs are designed to accomplish the following objectives: (a) only properly authorized changes are introduced to an information resource; (b) all such changes are tested before actual release; (c) the duties of change initiator, change approver and change implementer are separated as often as is practicable, given the Company's technology environment; (d) changes are planned and managed according to the level of associated risk; (e) changes should consider the potential impact on the performance and/or capacity of other technology components; (f) rights to modify the production environment are granted only on a "need to know/use" basis; (g) changes undergo technical and business compatibility testing with evidence retained; (h) testing is performed in a dedicated environment commensurate with test requirements and planned test activities; and (i) changes are accompanied by sufficient user training and appropriate procedural updates (version control) to the system.

3.0 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.

4.0 APPLICATION SCENARIO: To establish the proper context within which change control management becomes necessary, consider a working information system project, meaning one whose complete version has successfully navigated the system development life cycle (SDLC) process and is currently in general use. The need for change to the working information system project (or the perception thereof), triggers the start of the change control management process. A chronological progression of Propel's change control activities is shown below. It is important to note that approximately 75%

of change initiatives/requests originate with our clients; approximately 25% originate from within the Company.

5.0 PLANNING/TRIAGE/APPROVAL OFFICER (TAO)/INITIATOR ROLE: Change Control Management begins with vision, planning and a commitment to follow the Company's prescribed SOPs. It is the synergy of these three functions which yields the best opportunity for proper execution, which in turn serves to minimize disruptions, errors and unauthorized changes. At the inception of a change request, the Vice President-Application Architecture (VP-AA) normally sits atop the triage/approval function as the Triage Approval Officer (TAO). Serving as TAO requires a unique skill set which includes the possession of adequate training, experience and a thorough understanding of the Company's technological environment. Yet, equally important are another set of skills: the ability to organize, communicate, delegate, and motivate. In the VP-AA's absence or inability to serve as TAO, an equally qualified Chief Administrative Officer (CAO) assumes responsibility of the triage/approval process and serves as TAO. In fact, because of the CAO's education, experience and leadership skills and her similarly unique understanding of the Company's technological environment, the CAO serves as TAO whenever VP-AA is the "initiator" of a change request. This is an example of having a core competency in depth.

6.0 DOCUMENTING AND TRACKING CHANGE CONTROL PROCEDURES/AXOSOFT, LLC (Axosoft): Each change request should begin with an issue tracking ticket. Propel® uses the Axosoft software platform for its change management tracking function. Axosoft is available to the Company as hosted software and is described as a Software as a Service (SaaS) cloud computing model. With this software, the Company's TAO has an ongoing ability to check the status of a pending change request, as well as to always know its place within the initiator, approval, development, staging, testing, production and implementation/deployment phases. The Axosoft resource also preserves the accompanying required narrative relative to justification, etc.

7.0 CATEGORIZATION/RISK ASSESSMENT/CLASSIFICATION/DISCRETIONARY INVOLVEMENT OF THE INFORMATION SECURITY MANAGEMENT COMMITTEE: Upon receipt of the change request, the TAO uses his/her experience to see the big picture and first decide if the requested change should in fact be made. If so, the request is then categorized as falling into one of two categories: a) normal operations or b) coordinated operations. In conducting this risk assessment, the TAO considers the size of the requested change, its complexity, its impact upon related systems, how much source code is involved in the change, is the server affected (which of course makes testing more difficult) and finally, are there financial considerations in play (higher cost usually means higher risk, thus warranting caution). Keeping these factors in mind, the TAO draws upon the above referenced skillset to classify the change request. If it falls into the "normal operations" category, the TAO must then determine which of the Company's application developers should be assigned the project. If the request is classified as "coordinated operations" the TAO uses his/her discretion in whether to refer the request to the Information Security Management Committee for its recommendation. An ad hoc meeting can be quickly called, the result of which is a special plan for moving the request forward (if in fact it should be approved). If so, it is ultimately assigned to an application developer and thus begins the development phase.

8.0 TICKET FLOW/DEVELOPMENT PHASE/THE RELEASE FOLDER: IMPLEMENTER ROLE: The Axosoft "ticket" follows the request through its entire process and forms a record of the work, testing, approvals, etc. It should be noted that from a data security perspective, credentialed access is required before work can begin on the change request. Upon the work being performed, the application developer accesses the Company's "Release Folder" where he/she uses a document template to record the work performed/action taken. The application developer is aware that his/her notes, findings, results, comments, etc., form a part of the evidentiary change record which accompanies the change request moving forward. With the application developer's work completed, the template, ticket and entire change request file are returned to the TAO who approves the work product (if appropriate to do so) and forwards the entire file to one of the Company's testing coordinators for testing. This occurs within the staging environment.

9.0 STAGING ENVIRONMENT/TESTING: This sub-policy is designed to ensure that all changes are tested in a controlled environment prior to implementation, which serves to protect related systems from disruptions or functionality/usability failure. In short, testing yields quality, and as the change itself is tested, an equally important effort is made to assess the change's impact upon elements, systems not being modified. Testing serves to satisfy expectations that the requested change meets all design requirements, functions appropriately and meets design parameters before moving to the implementation phase. Specifically, the testing coordinator uses a standard suite of tests to discover any issues and ultimately to make the determination that no issues remain prior to implementation and deployment. If issues do remain, then the TAO is advised. Upon the TAO's review, and "fix" the ticket and entire record is again returned to the staging environment where further testing takes place to ensure that there are no unresolved issues. With this issue free result, the testing coordinator sends a status e-mail message to the "Deploy" team (Deploys) for information and update. The change request now moves to production via the account manager who serves as a member of Deploys.

10.0 ACCOUNT MANAGER/CLIENT APPROVAL WHEN NECESSARY/MOVE TO PRODUCTION PHASE/IMPLEMENTATION: At this juncture, the account manager makes his/her final review and communicates to the client that all work associated with the change request has been completed. This communication can be for client approval and/or as an informational update. Where the change request was initiated internally as opposed to being initiated by the client, or perhaps, because the nature of the change does not necessitate approval, the account manager simply reviews the change request work product, and if appropriate, advises the TAO that the work meets with his/her approval and further requests that the change be deployed to production. The Deploys are copied for informational purposes. Under normal circumstances the VP-AA will serve as the Company's implementation designee.

11.0 PRODUCTION PHASE/DEPLOYMENT BY VP-AA/COURTESY COMMUNICATION TO CLIENT: In cases where the client is neither asked for approval nor advised of changes (see Section 9.0 above) the client's only notification of deployment will be in the form of an e-mail message from the account manager who will pass along the implementation designee's anticipated window of time for deployment. Of course, clients who have been made aware of the change, will also receive an e-mail

deployment notification from the account manager. The VP-AA seeks to schedule deployment at a minimally inconvenient time window for the client.

12.0 TEMPLATE FOR ACCOUNT MANAGER'S DEPLOYMENT NOTIFICATION: Referencing Section 10.0 above, the following is a suggested template for the text of an account manager's e-mail notification to a client of a pending change deployment. The account manager is free to modify the text of this notification depending upon specific circumstances. "*Dear_____(client): I want to make you aware that on (date) between (start time) and (end time), Propel is planning to install/deploy an application upgrade to your Propel Platform and the system may be offline for this short period of time. All operations around the platform server will resume immediately following the maintenance window. Propel appreciates your patience and understanding. As always, if you have questions or concerns please let me know at your earliest convenience. Sincerely, (Account Manager)".*

13.0 VERSION CONTROL/DATA SECURITY: The Company maintains a version control system which is a client specific repository of source code files. On a client by client basis, each revision is tracked and automatically assigned a release/revision number. Further, each revision receives a timestamp, an identification of the team member making the revision as well as the required comment explaining why the change was made. The Company considers its ability to track changes (and if necessary, to reverse changes) as being critical to good change control management. From a data security perspective, it is important to note that the right to consult these files requires preapproved access based upon a need to know/use basis. Older versions of the changed application, etc., are maintained electronically for the life of the project.

14.0 FALLBACK PLAN: With a clear understanding of the Company's technical environment, each phase of the change control process is followed by testing and evaluation. Thus, as a practical matter, if such testing and evaluation indicate an undesirable result, a fallback/restoration plan can be more efficiently accomplished when it can occur incrementally, by phase. Should fallback/restoration be required, it is standard operating procedure (SOP) for either the VP-AA or Senior Application Developer (SAD) to execute the plan, which allows the application/system, etc., to safely return to its previous operating status.

15.0 COMMUNICATING CHANGES: Change initiators (especially clients) should be kept informed about the status of their request as well as adequate notice of system downtimes, if any. Of course, it is also important to schedule downtime(s) during a window which is least likely to cause inconvenience to users (see Section 11.0).

16.0 POLICY COMPLIANCE

16.1 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).

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

16.3 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.

17.0 RELATED STANDARDS, POLICIES AND PROCESSES

Please review the following policies for details about both protecting both Company and client information when working in a "change management" environment:

- *Propel Information Security Management Policy (ISMP)*
- *Propel Information Security Sub-Policy Number 3-Platform System Development Life Cycle (SDLC) Compliance.*

Revision History: Date	**Revision No.**	**Description of Changes**
12-15-2017	01	To formalize the Company's Change Control Management Process.
09-13-2018	02	To provide a more detailed roadmap of Propel's procedures in connection with change control.
02-23-2019	03	Standardize policy language to conform to other policies…no formal approval required for these changes.