Privacy and Security Policy

1 Introduction

One of the central functions of Leafsprout's software is secure and responsible stewardship over personal information, including personal health information. We are committed to protecting the security and confidentiality of the personal information entrusted to us and the personal information with which we come into contact, both in the course of our software's performance, and during setup and maintenance activities, as individuals.

This policy outlines Leafsprout's general approach to information privacy and security, and assigns the responsibilities for information security as well as for reporting and oversight.

2 Objective

The intent of Leafsprout's Privacy and Security Policy is to achieve the following:

- **Compliance with Laws and Regulations** pertaining to privacy and security of information – In Ontario this means compliance with Ontario's *Freedom of Information and Protection of Privacy Act*, 1990 ("FIPPA"), and Ontario's *Personal Health Information Protection Act*, 2004 ("PHIPA").
- **Ethical Practices** – Compliance with laws and regulations is a minimum standard for behaviour; Leafsprout aims to fulfil its role as a good corporate citizen in a broader sense, as this applies to information security.
- **Risk management** - Information security risks must be analyzed, treated and monitored throughout the organization.
- **Safeguarding of Information Assets** – Leafsprout safeguards information handled by our software, as well as information with which we come into contact as individuals, during the course of maintenance activities.
- **Accountability and Responsibility** – Accountability must be clearly defined and well understood.
- **Awareness** – An effective methodology is one that is used; in order for this to happen, all employees must be familiar with it.
- **Proactive Prevention and Response** – Participants must act in a timely and co-operative manner to prevent, detect and respond to security incidents.
- **Integration** – The various procedures and policies that make up Leafsprout's methodology regarding information security must work together in a coordinated fashion.
- **Reassessment and Continuous Improvement** - The security of information systems should be reviewed and reassessed at regular intervals to ensure that processes are streamlined and cohesive enough to be followed easily and consistently and to be a net benefit to the company, yet comprehensive enough to ensure the security they aim to provide.

3 Scope and Applicability

This policy is meant to provide guidance on Leafsprout's approach to information privacy and security. It may be supported by topic-specific policies, standards, and procedures. This policy applies to all activities and employees of Leafsprout, both in the process of producing our software, and during installation, maintenance and support of our software and deployments.

4 Policy Statement

Leafsprout acts to protect the confidentiality and integrity of information entrusted to our care.

We respect and comply with Ontario's Freedom of Information and Protection of Privacy Act, 1990 ("FIPPA"), and Ontario's Personal Health Information Protection Act, 2004 ("PHIPA"). We will not collect, use or disclose personal or health information in any manner that is not in accordance with FIPPA, PHIPA, or established company policies.

We safeguard the privacy and security interests of our customers and their clients as outlined below.

4.1 Education and Awareness

Leafsprout endeavours to foster an environment of awareness of and respect for the importance of privacy and security considerations. Employees shall be required to complete Leafsprout's privacy and security awareness training as specified in the Privacy and Security Education and Awareness Process within the first 30 days of employment at Leafsprout. Following the initial privacy and security training, periodic review shall be undertaken by all Leafsprout employees, also as outlined in the Privacy and Security Education and Awareness Process. The aim of periodic review is twofold:

- to provide a refresher on privacy and security policy, and to increase awareness;
- to draw out any insights that employees may have over time regarding improvements to Leafsprout's methodological or policy approach to privacy and security.

4.2 Classification and Risk Assessment of Information Assets

The company shall routinely identify and document information assets and determine any risks that may be associated with them. Mitigation strategies shall be established as appropriate, and associated mechanisms and ownership shall be assigned. All personal and personal health information, to the extent that this comes into the company's possession, will be classified as confidential and treated with the highest level of sensitivity.

4.3 Technology Within Software

Within our software we use a variety of mechanisms to safeguard the security of the system and the information handled by it. The appropriate use of these technological mechanisms is a subject that shall be scrutinized during code reviews as outlined in our Change Control Process. We work to ensure that the security mechanisms routinely used by Leafsprout, and expected during code reviews, reflect industry best practices.

4.4 Limited Access

There are instances where Leafsprout employees come into contact with client information – in particular this may occur during installation, data migration, troubleshooting and maintenance activities. During these occasions, access to Personal Information shall be limited to those employees and

contractors who reasonably require such access in order to provide products or services to customers or in order to do their jobs.

4.5 Monitoring and Reporting

On an annual basis, the Quality, Process and Regulatory Lead shall report to the CEO on the status of security and privacy endeavours within the company. This report shall include:

- a review of any and all information security incidents that have occurred during the past year and retrospective assessment of impact and significance, appropriateness of response that was made, as well as conclusions that may be drawn from this body as a whole, if any are appropriate;
- plans for the upcoming year re. privacy and security endeavours within the company;
- report on employee compliance with Privacy and Security Education and Awareness Process.

4.6 Incident Management

Leafsprout shall take appropriate remedial action to address non-compliance with its privacy requirements. This shall include:

- notifying the Quality, Process and Regulatory Lead of the incident or non-compliance.

Remedial action undertaken by the company may include:

- logging and addressing a high-severity defect report;
- immediate support to investigate and address any configuration issues that may be responsible for the incident;
- changes to policies, processes and procedures.

The consequences of non-compliance or failing to take appropriate remedial action may include invoking measures up to and including dismissal or termination of contract.

4.7 Complaints and Inquiries

The Quality, Process and Regulatory Lead, or designate, shall manage and respond to complaints, questions and feedback about Leafsprout's privacy practices.

Leafsprout shall review, investigate and document every complaint received and shall monitor for any trends arising as outlined in Section 4.5 Monitoring and Reporting.

If the sender provides contact information, Leafsprout shall:

- acknowledge the complaint, question or feedback within five (5) business days of receipt and provide information about any relevant internal and external complaint mechanisms;
- respond to the sender's question, feedback or complaint within thirty (30) business days of receipt; and
- notify the sender of its expected timeframe for response if a delay is anticipated.

Leafsprout shall take appropriate measures to respond to complaints and feedback, which may include changing company policies and practices.

5 Accountability: Roles and Responsibilities

The following roles are explicitly involved in realizing Leafsprout's privacy and security-related objectives:

CEO – oversees proper functioning of the company, and ensures that it is a good corporate citizen, respecting its obligations to society in general, and that it remains in good legal and regulatory standing according to the jurisdictions within which it operates. In relation to privacy and security, this involves providing guidance and oversight of the privacy and security risk management program. Appoints Quality, Process and Regulatory Lead. Reviews and approves company policies. Ensures that all the moving parts are working together harmoniously towards achieving the company's objectives re. privacy and security.

CTO – ensures that technologies in use within products are appropriate for meeting company objectives regarding standards, quality, regulatory, in particular for safeguarding private information entrusted to our software

Quality, Process and Regulatory Lead – develops and leads privacy, security, process-related, standards-related endeavours within company

All employees – respect and implement company policies, processes, procedures; support company objectives regarding privacy and security.

6 Reference and Associated Documents

The following documents are referenced within this policy:

- Ontario's Freedom of Information and Protection of Privacy Act, 1990 ("FIPPA")
- Ontario's Personal Health Information Protection Act, 2004 ("PHIPA")
- Leafsprout's Privacy and Security Education and Awareness Process

Document Control

The electronic version of this document is recognized as the only valid version.

Document Location	This document can be found in Leafsprout's document control system at: Leafsprout/Methodology/PrivacySecurityPolicy.pdf
Review Frequency	This document will be reviewed at least every two years.
Document Sensitivity	Publicly-available

Revision and Approval History

Author	Approver(s), Title(s)	Version	Date
Elizabeth Stark	Cezary Klimczak, CEO	1.1	Aug 17, 2013