TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

Incident Response Policy

Version: 1.0
Effective Date: 11/20/16

Author: Joshua Budman, Chief Technology Officer

Disclaimer: This policy was created by Tissue Analytics, Inc. for the sole use of its employees and clients.

Overview

Tissue Analytics, inc. (TA) is committed to swiftly and appropriately reporting and responding to all incidents related to software bugs, data breaches or data leaks. A proper response to any and all incidents, should they arise, will minimize any potential downstream effect of these incidents.

Purpose

The purpose of this policy is to establish standards for the incident response practices used by TA. Effective implementation of this policy will minimize the consequences caused by any incidents associated with TA's software in spite of TA's best efforts to prevent said incidents.

Scope

All employees, contractors, consultants, temporary and other workers at TA and its subsidiaries must adhere to this policy. This policy applies to employees or contractors employed by TA.

Policy

4.1 General Requirements

4.1.1 Any incidents concerning data breach or leakage must be reported to TA Information Security within 24 hours of the discovery of

said breach.
4.1.2 Any incidents concerning data breach or leakage must be reported to all TA clients within 7 days of the discovery of said breach.
4.1.3 Any incidents concerning data breach or leakage must be recorded internal to TA and a record of the issue plus the efforts TA took/will take to fix said issue must be presented to any TA client upon request.
4.1.4 TA establishes incident response practices in keeping with Request for Comments 2350 (RFC 2350).
4.1.5 Specifically, TA ensures secure communication for all incident response-related communication.
4.1.6 Additionally, once an incident is reported to Information Security, the incident is appropriately "triaged" and "coordinated" within Information Security. Information Security allocates responsibility for solving the incident to the individual most closely associated with the construction of the software that led to the incident. This responder is then overseen by Jason Hihn, TA's Chief Information Security Officer.
4.1.7 All client reported incidents can be directed to Joshua Budman (josh@tissue-analytics.com, Chief Technology Officer) or John Howay (john@tissue-analytics.com, Chief Information Security Officer). TA can be contacted by mail at the following address:

8 Market Pl. Suite 405
Baltimore, MD 21202

4.1.8 TA ensures a fully accessible channel of communication for client-initiated incidents in keeping with RFC 2350.

Policy Compliance

5.1 Compliance Measurement
The Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Information Security team in advance.

Related Standards, Policies and Processes

Definitions and Terms

Request for Comment 2350 (RFC2350): A specific publication from the Internet Engineering Task Force that mandates proper reporting of and response to software-related incidents.

Revision History

Date of Change	Version Number	Responsible	Summary of Change