Patch Management Policy

Version: 1.0
Effective Date: 04/25/17

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) routinely updates its software and submits new software patches in order to improve functionality and solve any bugs that may arise. TA ensures that it performs robust testing, quality assurance and documentation of any new software patches that are installed over the lifecycle of the software.

Purpose

The purpose of this policy is to establish standards for the patch management policy used by TA. Effective implementation of this policy will minimize the risk of any issues that may arise as a result of new software patches that are installed while the TA software is in use.

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 In keeping with Request for Comment 2196 (RFC2196) Subsection 6 point 1 TA will immediately install new software patches

in response to any reported incidents, which applies to both self-reported incidents and site-reported incidents.
4.1.2 Any applicable security-related patches produced by Amazon Web Services (AWS) will be obtained and installed as stated by RFC2196 subsection 6 point 2.
4.1.3 TA engages in daily monitoring of any anomalies related to new patches up to 7 days after they are released. If detected, TA will report and document said anomalies immediately in keeping with RFC2196 subsection 6 point 3.
4.1.4 TA system administrators are responsible for staying up to date with applicable software patches in keeping with RFC2196 subsection 6 point 5.
4.1.5 Individuals outside of Information Security, such as TA account managers, are responsible for regularly validating the compliance of current software patches with both TA and client site policies. This is in line with RFC2196 subsection 6 point 6.
4.1.6 TA maintains a clear and well-defined maintenance patch schedule, which will be provided to the client site upon request.
4.1.7 TA uses a top-5 patch management software and adheres to a strict alerting policy. TA employees are required to maintain rigorous documentation of any patches, including a clear explanation of the patch itself and a priority level of said patch. Patches are prioritized on a scale of "Very Low" to "Very High" with 5 distinct ratings.
4.1.8 Patches are addressed based on the priority they are given by TA. The table below summarizes the patch application time based on said patch's designated priority:

Priority	**Application Time**
Very High	1-3 Days
High	3-5 Days
Medium	7-14 Days
Low	15-31 Days
Very Low	1-2 Months

4.1.10 All patches undergo rigorous testing protocols before they are pushed to production. Additionally, patches must go through TA's quality assurance criteria before they are pushed to production.

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

- Penetration Test Report

Definitions and Terms

Request for Comment 2196 (RFC2196): A specific publication from the Internet Engineering Task Force that mandates proper patch management.

Revision History

Date of Change	Version Number	Responsible	Summary of Change
5/25/17	1.0	Joshua Budman	Removed penetration test reference