Anti-Virus and Anti-Spyware Policy

Version: 1.0
Effective Date: 10/07/16

Author: Joshua Budman, Chief Technology Officer

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

1.Overview

Anti-virus and anti-spyware software is used in order to protect the company's software, both internal and cloud-hosted, from harmful viruses that may acquired from external sources such as the World Wide Web. Airtight practices for protecting software from viruses ensure that all computers used by Tissue Analytics, Inc. (TA) are fully safe and secure. This is especially important since TA's servers, hosted on Amazon Web Services (AWS), contain patient protected health information (PHI) and internal devices connect to these servers.

2. Purpose

The purpose of this policy is to establish standards for the setup of the practices and/or anti-virus/anti-spyware protecting software on TA's computers. Effective implementation of this policy will minimize unauthorized or unwanted viruses/spyware on TA's computers.

3.Scope

All employees, contractors, consultants, temporary and other workers at TA and its subsidiaries must adhere to this policy. This policy applies to server equipment and any internal hardware equipment that is owned, operated or leased by TA or registered under a TA-owned internal network domain. TA employees' computers are administered by a TA systems administrator.

This policy specifies requirements for anti-virus or anti-spyware software to be installed on all TA operating systems, both internal and cloud-based.

4.Policy

4.1 General Requirements

4.1.1 Employees are not permitted to use personal devices for any TA-related functions.

4.1.2 Employees are expressly forbidden to install or use any software, including operating systems, that have not been approved by the CTO or senior systems administrator.

4.1.3 All TA-purchased devices must use the most recent, stable version of an approved Macintosh or Linux operating system as these OS' are significantly less virus-prone than Microsoft OS'.

4.1.4 Personal devices may, under no circumstances, be used for official TA business or be connected to the secure TA intranet.

4.1.5 Any TA-issued computer with an approved Macintosh OS must be equipped with the most recent version of avast! Antivirus for Mac prior to being used for work-related purposes. Linux OS machines are not required to have anti-malware software installed and this is up to the discretion of the employee user of said machine.

4.1.6 All cloud-based machines must use exclusively Linux OS'. However, due to the sensitivity of the data processed and maintained on TA's servers, TA requires that all cloud-based machines possess the most recent, stable version of Security for Amazon Web Services by BitDefender.

4.1.7 TA requires periodic anti-malware scans of all work machines, both internal and cloud-based.

4.1.8 All removable media must be checked for the presence of malicious software before use.

4.1.9 All external media, such as email attachments, must be employee-trusted before it is accessed. If any malicious programs are suspected to have emerged from such an action, this must be immediately reported to TA information security.

5. Implementation

In addition to the periodic scans discussed in the process section, any non-company-issued readable and writeable media is prohibited. The version numbers and update dates for each of the anti-malware products used are listed below:

Avast! Antivirus for Mac: Mac OS devices using avast! Must use version 11.17 or later. All devices were last updated in 9/2016.
BitDefender GravityZone: Server-side machines using BitDefender use BitDefender GravityZone and were last updated in 9/2016.

The most recent scan results (5/26/2017) are attached.

Compliance

6.1 Compliance Measurement

The TA Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner. Overall performance using a combination of methods: 1. Number of instances of malware reported by company employees and 2. Percentage of malware blocked by anti-malware software.

6.2 Compliance Management

All TA security policies are managed by the TA Information Security team, which consists of TA's Chief Technology Officer, Joshua Budman, and TA's Director of Software Engineering, John Howay. All management of antivirus policy adherence is conducted manually by conducting random checks of employee work machines and/or by collecting reports from employees on any suspicious software programs identified by said employees. TA conducts training related to this policy as part of new employee onboarding. TA also conducts semi-annual policy review for this policy. Please reference the attached spreadsheet for further detail on TA's management of anti-malware policies.

Measurement and management of these policies are illustrated using TA's anti-malware spreadsheet that is updated by a previously appointed systems administrator.

Revision History

Date of Change	Version Number	Responsible	Summary of Change
5/31/17	**1.0**	Joshua Budman	Changed annual review to semi-annual in section 6.2