Anti-Virus and Anti-Spyware Procedure Document

Version: 1.0
Effective Date: 11/11/16

Author: Joshua Budman, Chief Technology Officer

Disclaimer: This procedure document 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 be 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 procedure 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 protocol. This protocol 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.

4.Protocol

4.1 For TA Management/Systems Administration

4.1.1 Inform each employee of the personal device policy prior to their first day. Document and report to management any refusal to adhere to TA's anti-malware practices.
4.1.2 Designate an individual in this group that is responsible for overseeing anti-malware practices, including maintaining logs of periodic scans and ensuring all relevant hardware has fully updated anti-malware software installed.
4.1.3 Install the most stable, recent version of avast! Antivirus for Mac on all TA-issued Macintosh computers within 24 hours of each computer's purchase and prior to any TA employee using said hardware.
4.1.4 Install the most recent, stable version of Security for Amazon Web Services by BitDefender on each new Amazon Machine Image (AMI) immediately upon deployment of said AMI.
4.1.5 Set all anti-malware software to conduct scans at a frequency of once per week or greater. Log all results from said scans.
4.1.6 Malware detection procedure:

isolate machine from network,
log all detected malware/infections in detail,
document steps taken to mitigate detections, and
re-network machine only upon zero-detection scan.

If the systems administrator is unable to remove malware, decommission machine until further action can be taken.
4.1.7 Conduct quarterly interviews with a select group of employees to assess for adherence to anti-malware policy and level of intrusion to daily work functions caused by said policy.

4.2 For non-management/non-systems-administration employees

4.2.1 Take part in initiation related to anti-malware practices prior to starting employment at TA. Express any discomfort or disagreement with said practices prior to beginning work related functions.

4.2.2 Do not interfere with anti-malware software running in your computer's background. If you suspect a problem with said software, or said software is causing disruption to daily work-related functions, report the issue to TA management/systems administration.
4.2.3 Report any instances of suspicious software or suspected malware to TA systems administration immediately upon discovery.
4.2.4 In the case of a malware outbreak, cease all function on your work machine until TA management/systems administration has been alerted and the situation has been rectified by the appropriate malware software.

Revision History

Date of Change	Version Number	Responsible	Summary of Change