TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

Web Application and Server Security 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.

Overview

Unsecured and vulnerable web applications continue to be a major entry point for malicious threat actors. Ensuring that servers powering the web application used by Tissue Analytics, Inc. (TA) are fully safe and secure is especially important since said servers are involved in the storage of patient protected health information (PHI) and the web application is involved in presenting this information to the client. Thus, Tissue Analytics adheres to server and web design best practices to ensure the safety and security of its servers.

Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by TA. The second purpose of this policy is to establish standards for the design of web-based applications by TA. Effective implementation of this policy will minimize unauthorized access to TA's proprietary information and technology and client site data.

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 that is owned, operated or leased by TA or

registered under a TA-owned internal network domain.

This policy specifies requirements for equipment on the internal TA network. More specifically, for secure configuration of equipment external to TA on Amazon Web Services, see **AWS Security Policies** for the latest version of this whitepaper. Additionally, for secure configuration of equipment external to TA hosted by our individual clients, consult the specific client's information technology security policy.

Policy

4.1 General Requirements

4.1.1 All internal servers deployed at Tissue Analytics must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Information Security. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is require to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and operating system/version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date
- Configuration patches for production servers must follow the appropriate patch management procedures per the **Patch Management Policy.**

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the **Server Audit Policy***.*

4.1.3 TA performs semi-annual penetration tests of both web and mobile applications to ensure secure coding practices. Results from the most recent penetration test, conducted in 08/2015, are contained in the **Penetration Test Report.**

4.1.4 TA developers responsible for developing the web and mobile applications must adhere closely to Open Web Application Security Programming (OWASP) methodology and Systems Development Lifecycle (SDLC) secure coding practices.

4.1.5 TA employs rigorous server hardening to defend against sensitive data exposure, security misconfigurations and missing function level access control.
4.1.6 Any TA web application component that is in production must meet or exceed the Community Emergency Response Teams (CERT) Malicious Content Mitigation Guide for Web Developers.

4.2 Configuration Requirements
4.2.1 Operating System configuration should be in accordance with approved Information Security guidelines.
4.2.2 Services and applications that will not be used must be disabled where practical
4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
4.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements. See the **Patch Management Policy** for more details on this.
4.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
4.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
4.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec)
4.2.8 Servers must be physically located in an access-controlled environment.
4.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring
4.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week
- Monthly full backups will be retained for a minimum of 2 years

4.3.2 Security-related events will be reported to Information Security,

who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host

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.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Server Audit Policy
- AWS Security Policy
- Individual Client's Information Technology Security Policy
- Patch Management Policy
- Penetration Test Report

Definitions and Terms

- **Amazon Web Services (AWS):** A collection of remote computing services that together make up a cloud computing platform, offered over the Internet by amazon.com.
- **Open Web Application Security Project (OWASP):** An online community dedicated to web app security.
- **Systems Development Lifecycle (SDLC):** a conceptual model used in project management that describes the stages involved in an information system development project, from an initial

feasibility study through maintenance of the completed application.

- **Community Emergency Response Teams (CERT):** Expert groups that handle computer security incidents.
- **Server Hardening:** Process of enhancing server security through a variety of means resulting in a more secure software environment.

Revision History

Date of Change	Version Number	Responsible	Summary of Change