TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

Server Audit Policy

Version: 1.0
Effective Date: 11/18/16

Author: Joshua Budman, Chief Technology Officer

Overview

See purpose.

Purpose

The purpose of this policy is to ensure all servers deployed at Tissue Analytics, Inc. (TA) are configured according to the TA security policies. Servers deployed at TA shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Ensure conformance to TA security policies

Scope

This policy covers all servers owned or operated by TA This policy also covers any server present on TA premises, but which may not be owned or operated by TA.

Policy

TA hereby provides its consent to allow TA Information Security to access its servers to the extent necessary to allow TA Information

Security to perform scheduled and ad hoc audits of all servers at TA.

4.1 Specific Concerns

Servers in use for TA support critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability or integrity of these systems.

4.2 Guidelines

Approved and standard configuration templates shall be used when deploying server systems to include:

- All system logs shall be maintained and sent to a central log review system
- All Sudo / Administrator actions must be logged
- Use a central patch deployment system
- Host security agent such as antivirus shall be installed and updated
- Network scan to verify only required network ports and network shares are in use
- Verify administrative group membership
- Conduct baselines when systems are deployed and upon significant system changes
- Changes to configuration template shall be coordinated with approval of change control board

4.3 Responsibility

TA Information Security shall conduct audits of all servers owned or operated by TA. Server and application owners are encouraged to also perform this work as needed.

4.4 Relevant Findings

All relevant findings discovered as a result of the audit shall be listed in the TA tracking system to ensure prompt resolution or appropriate mitigating controls.

4.5 Ownership of Audit Report.

All results and findings generated by the TA Information Security Team must be provided to appropriate TA management within one week of project completion. This report will become the property of TA and be

considered company confidential.

Policy Compliance

5.1 Compliance Measurement

TA Information Security shall never use access required to perform server audits for any other purpose.

TA will verify compliance to this policy through various methods, including but not limited to, 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 TA 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

None.

Definitions and Terms

None.

Revision History

Date of Change	Version Number	Responsible	Summary of Change