TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

Simple Mail Transfer Protocol (SMTP) Server Configuration Policy

Version: 1.0
Effective Date: 11/18/16

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

Vulnerable Simple Mail Transfer Protocol (SMTP) servers are a major entry point for malicious threat actors. Ensuring that servers 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). Thus, Tissue Analytics adheres to SMTP server design and protection 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 SMTP server equipment that is owned and/or operated by TA. Effective implementation of this policy will minimize unauthorized access to TA's proprietary information and technology as well as any client-associated PHI.

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 *Amazon Web Services: Overview of Security Processes* by consulting http://aws.amazon.com/security/ for the latest version of this whitepaper. For specifics on the AWS SMTP Server Protocol one can consult https://aws.amazon.com/ses/faqs/.

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 changes for production servers must follow the appropriate change management procedures

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

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved Information Security gudielines.

4.2.2 SMTP Server must act as a relay exclusively between the Internet and the Internet Mail

4.2.3 SMTP Server inspects content per AWS Simple Email Service best practices

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

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

- Server Audit Policy
- Web Application Development Policy

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.

Revision History

Date of Change	Version Number	Responsible	Summary of Change