Backup and Disaster Recovery Policy

Version: 1.0
Effective Date: 11/10/16

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

Machines that are responsible for storing/transferring sensitive data are susceptible to damage or corruption, despite all safeguards put into place preventing such events. Having proper backup and disaster recovery protocols in place in cases of damage or destruction to critical equipment is essential for ensuring that Tissue Analytics, Inc. (TA) can continue to service its customers without significant interruptions in service.

Purpose

The purpose of this policy is to establish standards for the backup and disaster recovery protocols utilized by TA in the case of damage to any business critical equipment. Effective implementation of this policy will minimize interruptions in service as they relate to damage of essential equipment.

Scope

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

This policy specifies requirements for equipment owned or leased by TA that stores or transfers data essential to its clients' use of the TA software.

Policy

4.1 General Requirements

4.1.1 All TA production servers kept on Amazon Web Services (AWS) responsible for the storage and/or transit of protected health information (PHI) or critical data, which constitutes data required for usage of the TA software, must be backed up in a geographically disparate location.

4.1.2 All TA production servers on AWS must be equipped with an automated failover mechanism (e.g. Elastic Load Balancing) to minimize downtime in the case of a disaster.

4.1.3 TA information security personnel must be alerted within half an hour about any potential damage sustained to TA's critical equipment caused by a disaster.

4.1.4 All data/databases must be backed up on a daily basis.

4.1.5 All production code must be backed up on a semi-weekly basis.

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.

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.
- **Elastic Load Balancing:** A service built-in to AWS that allows for automated traffic redirection to healthy servers in cases of high user volume.

Revision History

Date of Change	Version Number	Responsible	Summary of Change