Information Security Policy

1. Policy Statement

Tons of Trash maintains electronic information resources that are essential for the operation of company business and collection of accounts receivable. These resources are valuable assets, over which Tons of Trash has both rights and obligations to manage, protect, secure, and control. Employees, vendors and clients are expected to utilize these resources for appropriate purposes, protect access to them, and control them appropriately. Examples of information resources include, but are not limited to, computer systems, network systems, software and data.

2. Purpose

This policy sets forth the mechanisms by which data stored on Tons of Trash owned/licensed computing systems and utilized by its employees, client, etc. is secured and protected. This policy is adopted and promoted in order to:

1. Meet record-keeping and reporting obligations as required by state and federal law.
2. Consistently maintain data integrity and accuracy.
3. Ensure that authorized individuals have timely and reliable access to necessary data.
4. Ensure that unauthorized individuals are denied access to computing resources or other means to retrieve, modify or transfer data.

Every employee must be aware of these risks, and act in a way to protect the information resources at Tons of Trash

3. Scope

This policy applies to all individuals associated with Tons of Trash, including, but not limited to:

- employees
- vendors
- clients

This policy applies to all Tons of Trash owned/licensed information technology hardware and its software, including, but not limited to, desktop workstations, mobile devices and Internet connectivity, such as:

- servers
- personal computers
- company owned smart phones
- network systems
- computer integrated telephony
- recorders
- other technology hardware

Tons of Trash Risk Management (Threats):

- Firewalls are regularly updated to the latest version.
- Software is downloaded only when approved by management.
- External vulnerability scans are performed on a regular basis.
- Virus and malware protection are installed on every desktop & mobile device. Scans and live updates are performed weekly.
- Removable media (CD's, USB drives) will not leave or enter Tons of Trash offices without approval of management.
- All data must be encrypted when transferring files.
- Employees are restricted to access unapproved internet sites.
- Un-authorized e-mail access is prohibited.
- All e-mails are scanned for viruses prior to download by our internet service provider. Any suspect e-mails are quarantined.
- System back-ups are performed daily.

4. Responsibilities for Information Security

Tons of Trash may designate one or more individuals as Information Security Officers with primary responsibility for assisting in matters pertaining to this policy. Every employee is responsible for protection of Tons of Trash assets, including information systems equipment and data. Each employee is responsible for notifying their supervisor whenever he or she observes an action that seems contrary to this policy. The Information Security Officer is responsible for responding appropriately to violations of the Information Security Policy.

5. User Identifications and Passwords

The System Administrator maintains all user-ids. Inactive user-ids are disabled. Users are required to change passwords every 90 days. Tons of Trash enforces password complexity by requiring a minimum length of eight characters and must contain at least two letters and one non-letter.

It is the responsibility of employees to confidentially maintain their user-ids and passwords in a secure environment. Employees who maintain several user-ids and passwords utilize a password vault on their personal computer. The approved password vault is KeePass.

No one should access the Collection Resource System or other systems without an authorized user identification code and password. Receiving a user-id requires approval from management. Modification to system access requires approval from management. User-ids may be revoked or disabled to protect the system at any time.

User-ids are immediately disabled when the employee's relationship is terminated with Tons of Trash. Managers and the employee's supervisor shall conduct exit interviews with departing employees whenever possible. All previously issued keys and access devices shall be collected, and any employee specific passwords or access codes shall be confirmed. The location of client data and

other confidential information in that employee's possession or control will be ascertained and reviewed, secured, or deleted as necessary.

6. Policy Awareness

Every employee at Tons of Trash signs a confidentiality agreement upon hiring. Each employee is given a copy of the Information Security Policy and is made aware of the importance of information systems security and their responsibilities in the process. Contracts are signed with vendors and clients, which include portions of the Information Security Policy.

7. Access to Equipment

Tons of Trash is SSAE 16 compliant as we utilize InMotion Web Services for all require cloud services on an as needed basis. All collection information and systems are stored in AWS SSAE 16 certified datacenters and protected against fire, water, physical damage and theft.

- 24x7 security guard and staff monitoring
- Video camera surveillance and recording
- Biometric security systems
- Multiple security checkpoints
- Keycard entries throughout the data center
- Minimum six month recording of video and access logging

8. Access to Data

Access to our LAN through ISP is firewalled by a router. Only authorized users are permitted access through a VPN connection. VPN access is only permitted by secure user-id and password. No other access is granted. External vulnerability scans are conducted on a regular basis. If file transfer is required for we utilize SFTP.

Sensitive data and program files are protected against unauthorized reading and copying.

9. Violations

Employees shall immediately report all known or suspected violations of policy or procedure to their immediate supervisor. Vendors or clients should report all known or suspected violations to Tons of Trash. Violations of this policy incur the same type of disciplinary measures as violations of other Tons of Trash policies.

- Document misconduct in employee personnel records
    - A description of the violation and the policy that was violated
    - Time and date of the violation

- Management will enforce the appropriate disciplinary action.
    - Verbal Warning
    - Written Warning
    - Employee Termination
    - Criminal Action

10. Revisions

Tons of Trash Information Security Policy is reviewed on a quarterly basis. All employees are encouraged to correspond with the Information Security Officer(s) regarding any suggestions for revising this document.