Saveology, LLC
Acceptable Use Policy

Approved By: Steve La Peruta Director of Information Technology Date 01/07/2010	**PCI Policy # 1010 Version # 1.0** **Effective Date:** 01/07/2010 **Revision Date: 1.0**

1.0 Purpose:

The purpose of this policy is to help protect **Saveology, LLC** and its workforce members from liability and business interruptions due to inappropriate use of IT resources and breaches of computer security. This policy outlines the acceptable use of computer equipment at **Saveology, LLC**. These rules are in place to protect the workforce members and the company. Inappropriate use exposes **Saveology, LLC** to risks including virus attacks, compromise of network systems and services, legal issues and business interruption.

2.0 Scope:

This policy applies to all **Saveology, LLC** workforce members, users, contractors, consultants, temps, and other workers (herein termed "users") using **Saveology, LLC**-provided IT resources described herein in their assigned job responsibilities.

This policy also applies to all equipment that is owned or leased by **Saveology, LLC**.

3.0 Policy:

3.1 Acceptable Uses:

a. Users will be permitted access to computer resources upon approval by the appropriate department director or supervisor.

b. Users must have no expectation of privacy as to any communication on or information stored within IT resources. Because of the need to protect the **Saveology, LLC** resources, the confidentiality of information stored on any computer device belonging to **Saveology, LLC** is not guaranteed.

c. Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, users must consult their supervisor or manager. Such use must not interfere with a user fulfilling his or her job responsibilities, interfere with other users' access to resources, or be excessive as determined by management. Any personal use of **Saveology, LLC's** resources must not result in significant added costs,

disruption of business processes, or any other disadvantage to **Saveology, LLC**.

d. For security and network maintenance purposes, authorized **Saveology, LLC** workforce members may monitor equipment, systems and network traffic at any time.

e. **Saveology, LLC's** IT resources will be audited on a periodic basis to ensure compliance with this policy.

f. Workforce members must take all necessary steps to prevent unauthorized access to confidential information, specifically cardholder data.

g. Sharing user identification and/or password information with any other person is strictly prohibited.

h. Keep passwords secure. Authorized users are responsible for the security of their passwords and accounts. All user level passwords must be changed every 90 days.

i. All PCs, laptops and workstations must be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended.

j. Because information contained on portable computers is especially vulnerable, special care will be exercised.

k. Postings by users from an **Saveology, LLC** email address to newsgroups must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of **Saveology, LLC**, unless posting is in the course of business duties.

l. All hosts used by the user that are connected to **Saveology, LLC** IT resources, whether owned by the user or **Saveology, LLC**, shall be continually executing approved virus-scanning software with a current virus database.

m. Users must use extreme caution when opening unexpected e-mail attachments received from any sender, which may contain viruses, e-mail bombs, or Trojan horse code.

n. User access privileges will be granted on a need-to-know (least privilege) basis.

3.2 Unacceptable Uses:

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing **Saveology, LLC** IT resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by **Saveology, LLC**.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or end user does not have an active license is strictly prohibited.

c. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management must be consulted prior to export of any material that is in question.

d. Introduction of malicious programs into **Saveology, LLC** IT resources (e.g., viruses, worms, Trojan horses, root kits, etc.).

e. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

f. Using **Saveology, LLC** IT resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

g. Making fraudulent offers of products, items, or services originating from any **Saveology, LLC** account.

h. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

i. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

j. Port scanning or security scanning is expressly prohibited unless granted prior authorization by the IT Security Manager

k. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.

l. Circumventing user authentication or security of any host, network or account.

m. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).

n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

o. Providing information about, or lists of, **Saveology, LLC** users to outside parties.

p. Sending unencrypted cardholder’s account numbers in email.

q. Unauthorized use of any instant messenger programs (i.e. AIM, Microsoft Messenger, Trillion etc), personal profile spaces (including MySpace, Facebook, Hotmail, Match, etc.) or file sharing (peer-to-peer) software.

r. Example of Prohibited Email and Communications Activities:
   - Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
   - Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
   - Unauthorized use, or forging, of email header information.
   - Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
   - Sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/ Extranet.

- Providing information about, or lists of, **Saveology, LLC** users to outside parties.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within **Saveology, LLC's** networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by **Saveology, LLC** or connected via **Saveology, LLC's** network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.0 Responsibility:
The Security Officer is responsible for leading compliance activities that bring **Saveology, LLC** into compliance with the PCI Data Security Standards and other applicable regulations.

5.0 Compliance:
PCI DSS Requirements 4 and 7

6.0 Forms(s):
None

7.0 Definition(s):
Definitions for technical terms are in Appendix A of the TurboPCI Easy™ Workbook.

8.0 Policy History:
Initial effective date: 01/07/2010

I have read and understand this Acceptable Use Policy.

_____
Print Name / Title

_____ _____
Signed Date

Witnessed by:

_____
Print Name

_____ _____

Signed Date