Acceptable Use
Version 3.2

1. Purpose

1.1. The company's network administration needs to provide a reasonable level of privacy for customers and employees. Improper use of the Internet and computers exposes the company to unwanted traffic and attacks.

1.2. All employees and third party users are expected to exercise good judgment to protect themselves and the company from undesirable activity.

2. Scope and Responsibility

2.1. Customers have a non-negotiable expectation of privacy and fair treatment. Employee compliance with this policy will ensure the entire company meets those expectations.

2.2. All employees and third parties, such as contractors and vendors, are responsible for adherence to this policy.

3. Policy

3.1. Password sharing is not allowed for any reason you may use only your own user name and password and you are to keep it secret. You may not accept someone else's pass word or use their session after they have logged on.

3.2. Only authorized employees may use credit card processing software or systems.

3.3. System and Network Activities – The following activities are strictly **prohibited**, with no exceptions:

3.3.1. Storage of credit card account numbers (PAN's) on local computers under ANY circumstances including spreadsheets and word documents.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.3.2. Credit card processing terminal(s) shall only be used as follows:

3.3.2.1. Processing sales and credits for our business only. Never process a transaction for another business for any reason.

3.3.2.2. You must be authorized by management to use the terminal(s).

3.3.2.3. Settlement of transactions is performed only by authorized personnel.

3.3.3. Cutting and pasting PAN's is prohibited, as this copies them to your computer's clipboard and, as such disables their protection.

3.3.4. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

3.3.5. Exporting software, technical information, encryption software or technology; in violation of applicable federal and state statutes.

3.3.6. Using or installing any unapproved hardware, such as a disk or USB Drive you brought from home or received from someone else, on a company computer.

3.3.7. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.) shall be prevented.

3.3.8. Causing security breaches or disruptions of network communication.

3.3.9. Port scanning or security scanning except by authorized personnel or contractors.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.3.10. Executing any form of network monitoring which will intercept data not intended for employee use, unless this activity is a part of an employee's normal job/duty.

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

3.3.12. Launching attacks on other computers or networks, for example, denial of service attacks.

3.3.13. 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.

3.3.14. Providing information about, or lists of, employees to outside parties.

3.3.15. Providing information about the company's systems or security precautions to unauthorized parties inside or outside the company.

3.3.16. Navigating to pornography, gaming or any other website for non-business purposes.

3.4. Email and Communications Activities – Only company authorized technologies shall be used to communicate credit card information. The following activities are strictly prohibited, with no exceptions:

3.4.1. Opening email links or attachments that are from any unknown person or organization or appear to be inauthentic or solicit you to open a "very important" attachment or link.

3.4.2. 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).

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.4.3. Sending unencrypted credit card numbers in email or other communication forms such as instant messaging.

3.4.4. Saving email received with credit card numbers. Email with credit card numbers must be printed out and immediately deleted.

3.4.5. Using social media such Facebook for sending or soliciting credit card information.

3.4.6. Using SMS or any form of text messaging to communicate credit card information.

3.4.7. Using any insecure messaging technology to communicate credit card information.

4. Enforcement

4.1.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Records

5.1. Appendix A – List of Authorized Users

6. Definitions

6.1. *Spam* - Unauthorized and/or unsolicited electronic mass mailings.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Appendix A: List of Authorized Users

Name of System/Application/Device	Name of Employee	Authorized Activities

Authorized by: _____

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.