Acceptable Use Policy
Version 01, April 2, 2008
Provided by: CSRSI

This is a sample policy from the PCI TOOLKIT®. The PCI TOOLKIT® is a web based program which leads the merchant through PCI compliance in an easy, understandable manner.

The PCI TOOLKIT® is sold through various Acquirers, Financial Institutions and merchant service resellers. Merchants need to contact their credit card provider to gain access to the PCI TOOLKIT®.

Features of the PCI TOOLKIT® include:
- Written in plain language
- Strong emphasis on education
- Thousands of merchants use the PCI TOOLKIT® every month for their PCI DSS compliance needs.

See more at www.pcitoolkit.com or www.csrsi.com.

1. Purpose

1.1. The company's network administration needs to provide a reasonable level of privacy for our customers and employees. Improper use of the Internet and our 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. Our customers have non-negotiable expectations of privacy and fair treatment. Employee compliance with this policy will ensure that 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. System and Network Activities – The following activities are strictly prohibited, with no exceptions:

3.1.1. Storage of credit card account numbers (PAN's) on local computers under ANY circumstances.

3.1.2. Cutting and Pasting PAN's as this copies them to your computers clipboard and, as such disables their protection.

3.1.3. Violations of the rights of any person or 1coname protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

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

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

3.1.6. Revealing your account password to others or allowing use of your account by others.

3.1.7. Effecting security breaches or disruptions of network communication.

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

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

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

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

3.1.12. 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.

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

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

3.2. Email and Communications Activities - The following activities are strictly prohibited, with no exceptions:

3.2.1. 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).

3.2.2. Sending unencrypted credit card numbers in e-mail or other communication forms such as instant messaging.

3.2.3. Save e-mail received with credit card number. E-mail with credit card numbers must be printed out and immediately deleted.

3.3. Enforcement

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

4. Definitions

4.1. Spam - Unauthorized and/or unsolicited electronic mass mailings.