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.

Incident Policy
Version 01, April 2, 2008
Provided by: CSRSI

1. Purpose

1.1. The purpose of this policy is to provide a framework for responding to the theft, loss or compromise of credit card information, collectively known as incidents.

2. Scope and Responsibility

2.1. Management shall appoint an Incident Response Team. This team and each member's role shall be documented on Appendix A to this policy, Incident Response Team Contact List.

2.2. Anyone discovering or suspecting a breach or unauthorized access to credit card information shall notify chairman of the Incident Response Team immediately.

2.3. If the chairman is not available, his/her designee is to be notified immediately.

3. Policy/Procedure

3.1. The following items are considered incidents:

3.1.1. Theft or loss of paper records containing credit card information.

3.1.2. Theft or loss of electronic media or devices containing credit card information.

3.1.3. Successful intrusion attempts whether discovered or reported through alerts from monitoring systems.

3.2. If a breach is discovered or suspected, take immediate action as follows:

3.2.1. Remove the affected computer from the network by disconnecting its cable.

3.2.2. Do not turn the machine off, log on to it or modify it in any way.

3.2.3. Notify the Incident Response Team Chairman.

3.2.4. Identify the path of the breach and block it, if possible.

3.2.5. If using wireless – Change the SSID

3.2.6. Preserve all logs and data.

3.2.7. Log all actions taken on Appendix B: Breach Log.

3.3. Incident Response Team actions.

3.3.1. Determine the extent of the breach.

3.3.2. Make required notifications according to local, state and federal laws and your merchant services contract.

3.3.2.1. You are required to notify your merchant bank within 24 hours of discovering or suspecting a breach.

3.3.3. Refer to http://www.visa.com/cisp and http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html for guidance on handling the breach.

3.3.4. Follow all instructions received from the merchant bank without delay.

3.4. Incident response plan must be tested annually.

3.5. A review of incidents and tests is to be conducted to identify improvement opportunities to this plan.

4. References and Cites

4.1. PCI Data Security Standard v1.1

5. Records

5.1. Incident Response Policy Appendix A: Incident Response Team Contact List

5.2. Appendix B: Breach Log

6. Definitions

6.1. SSID – The name of the wireless network that is to be changed in the event of a breach.

Incident Response Policy Appendix A: Incident Response Team Contact List

Name of Member	Telephone Number

Name and Phone number of Merchant Bank:

Incident Response Policy Appendix B: Breach Log

Date of discovery: _____

Actions taken – note date and time of each action:
