Incident Policy
Version 3.2

Implementation Notes

Incident response is a critical need for every business, large or small. When developing your specific response you should consider all aspects of your business, whether it is the warehouse or the accounting office, any incident can hamper your ability to operate. Other facilities can affect your relationship to the payments space. If you can't deliver your product, you can't take orders. Likewise if your call center burns down and you can't take the orders, you can't deliver any products.

When preparing your plan consider all of the plausible events, they may be earthquakes, floods, fire, etc. Being prepared will reduce confusion in case an incident does occur. Remember that if there is a general emergency, you will need a plan to locate and assist your employees. An employee who doesn't have a place to live or is worried about his/her family may not be able to come to work and your business may suffer.

Additional, company policies or procedures will need to be written to address the specific needs of the company. In particular you must write the aforementioned incident response plan that takes into account all of your facilities.

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.

Incident Policy
Version 3.2

1. Purpose

1.1. The purpose of this policy is to provide a framework for responding to unauthorized access to the network and 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 in Appendix A to this policy, Incident Response Team Contact List.

2.2. Management shall develop a specific incident response plan tailored to the needs of the business.

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

2.4. 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.

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.

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

3.1.4. Theft or loss of a Point of Sale Terminal or credit card machine.

3.1.5. Discovery of any unauthorized wired or wireless device.

3.1.6. Destruction or compromise of company facilities, computers or network equipment.

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 in Appendix B: Breach Log.

3.3. Incident Response Team actions.

3.3.1. Determine the extent of the breach.

3.3.2. Notify executive management.

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.

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

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

3.3.4. 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.

3.3.5. 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 v3.2

5. Records

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

5.2. Incident Response Policy 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.

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.

Incident Policy
Version 3.2

Incident Response Policy Appendix A: Incident Response Team Contact List

Name of Member	Role	Telephone Number
	Chairman	

Name and Phone number of Merchant Bank:

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.

Incident Policy
Version 3.2

Incident Response Policy Appendix B: Breach Log

Date of discovery: _____

Actions taken – note date and time of each action:

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.