Policy Management and Training
Version 3.2

1. Purpose

1.1. The purpose of this policy is to define the requirements for policy management and training.

1.2. These requirements are designed to minimize exposure to the company from the loss of credit card information and comply with the Payment Card Industry Data Security Standard (PCI).

2. Scope and Responsibility

2.1. This policy is implemented by the Information Department.

2.2. All employees are required to adhere to this policy.

2.3. Write additional policies and procedures to address the specific circumstances of your business.

3. Policy

3.1. Policy Implementation

3.1.1. Policies must be approved by Change Control and Review Committee prior to implementation.

3.1.2. Approved versions of all policies will remain in effect until a new version of the policy is approved.

3.2. Training

3.2.1. All employees must read all policies that apply to their job responsibilities.

3.2.1.1. The training module of the PCI ToolKit may be used in place of the manual records in the next step. Using the PCI ToolKit for training allows employees to

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.

train and test, then the ToolKit automatically records and manages training qualifications and activities, or;

3.2.1.2. A record shall be maintained for each employee indicating the employee has read and understood each policy they are required to read. See Attachment A for Training Record.

3.2.2. Employees must be made aware of and must read and acknowledge new versions of policies as they are implemented.

3.3. Third Parties

3.3.1. All third party resources must read all policies that apply to their responsibilities.

3.3.2. A record shall be maintained for each third party resource indicating they have read and understood each policy they are required to read.

3.3.3. Third parties must be made aware of and must read and acknowledge new versions of policies as they are implemented.

3.3.4. All contracts, statements of work and other agreements with third parties must include the requirement for third parties to comply with PCI and card association security standards. In addition vendors must agree that they will maintain PCI compliance at all times while in possession of your data

3.4. Security Awareness

3.4.1. A security awareness program including information on handling credit cards and credit card information must be

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.

conducted annually for all employees and third party system users.

3.5. Annual Review

3.5.1. All policies must be reviewed annually and updated as required to satisfy current requirements.

4. Enforcement

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

4.2. External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5. Records

5.1. Appendix A: Policy Training Record

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.

Policy Management and Training
Version 3.2

Appendix A: Policy Training Record

Name: _____

Signing on the lines below acknowledges that you have read and understand the referenced policy.

Policy Name	Policy Version	Signature	Date

Instructions:
For each required policy, list the policy name and version in the table below. You must read the policy and sign and date on the associated policy line. New versions of policies require a separate line in the table above.

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.