Credit Card Processing – IP Terminals
Version 3.2

Requirements for Use of this Policy

- This policy may only be used if your business meets **all** of the following requirements:
  - Your business accepts Credit Cards using only a stand-alone point of sale terminal(s), and;
  - The terminal is an approved stand-alone Point of Interaction Device connected to the internet, and;
  - You NEVER transmit cardholder data over a network of any kind, either internal or external, other than through the terminal and;
  - Your business NEVER stores cardholder data in any electronic form. This includes spreadsheets, word documents and any place else in any computer anywhere - ever, and;
  - IF you store credit card information you only store it on paper, and;
  - IF you receive any credit card information (Card number, expiration date, cardholder name and/or other credit card information) that you only receive it on paper and it is not ever sent to you electronically.

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.

Credit Card Processing – IP Terminals
Version 3.2

1. Purpose

1.1. This policy is written to ensure the proper controls are in place to protect the security of our customers and business by keeping our customer's credit card information secure.

2. Scope and Responsibility

2.1. The following devices are covered:

2.1.1. The terminal(s) is an approved stand-alone Point of Interaction Device connected to the internet.

2.2. All employees are responsible for following the requirements of Section 3.4

2.3. Managers are responsible for implementing the requirements of all sections.

3. Policy

3.1. Electronic storage of credit card information is strictly prohibited in any form. This includes spreadsheets, computers, mobile devices and any other electronic device.

3.2. Credit card information may only be entered into credit card processing terminals.

3.3. Rules Governing Terminals

3.3.1. Credit card terminals, if using a telephone connection, shall not be connected to a voice over IP (VOIP) telephone system. VOIP makes a telephone connection extremely insecure, as it exposes transmissions to the public Internet.

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. Terminals shall run current software. Check with your provider or bank if you are unsure of your software currency.

3.3.3. Employees must have a reference so that they can inspect the terminals at the start of each shift. This reference may take the form of photographs, nameplate information, serial number and/or a guide for what to look for.

3.3.4. Any maintenance or equipment changes are to be pre-arranged and verified with your merchant services provider by calling them at a phone number that is known to you. Incoming calls may not be the sole basis for allowing anyone to work on or exchange the terminal(s).

3.3.4.1. Employees shall be instructed not to allow anyone who has not been authorized by management to have access to any terminals

3.4. All Employees

3.4.1. At the start of each shift:

3.4.1.1. Inspect the terminal(s) and any PIN Pads to verify that;

3.4.1.1.1. It is the same terminal as originally delivered to the business. This can be verified verifying the terminal has the correct serial number and information sticker from the original delivery, and;

3.4.1.1.2. Physically inspect the terminal to ensure that there are no overlays or objects inserted into the swipe path. Inserted objects and overlays may be devices intended to capture and steal credit card information and or personal identification numbers (PINs), and;

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.

3.4.1.1.3. Inspect the area around and above the machine to make sure that there are no unauthorized devices such as cameras that may have been placed nearby to capture video or sound from transactions.

3.4.1.1.4. If you do find evidence or even suspect there has been tampering:

3.4.1.1.4.1. Do not use the terminal.
3.4.1.1.4.2. Lock it up in a secure place.
3.4.1.1.4.3. Call your manager.
3.4.1.1.4.4. Call your merchant services provider for instructions.

3.4.1.2. Never allow anyone to use, modify or replace the credit card terminal unless you have been notified in advance of the service and that notification has been verified by calling your merchant services provider at the number from YOUR records. Do not rely on or allow the person performing the service to participate in the verification.

3.4.2. Credit card information may never be stored electronically. This includes spreadsheets, word documents and any place else in any computer anywhere

3.4.3. Keep the credit card terminal out of reach and away from members of the public and unauthorized employees.

3.4.4. Observe the Security Awareness Training and Program.

3.4.5. Order forms and receipts with credit card numbers printed on them shall be secured by placing in a cash drawer or a locked file when not in use.

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.

3.4.6. Management approval must be obtained prior to removing any paper records containing credit card information from secured areas.

3.4.7. All paper records containing credit card information must be clearly identified as Classified.

3.4.8. Under no circumstances shall the security code, which is sometimes called the CVV or CVC value, be written down or collected on paper. This number is found printed on the signature block of the card on MasterCard, Visa and Discover and printed on the front of American Express cards.

3.4.8.1. Employees may collect this value directly from a card or verbally from the cardholder over the phone. It may be entered directly into the terminal only.

3.4.9. Cards may never be swiped into devices other than the credit card terminal.

3.4.10. If paper records must be sent outside of the facility or another internal facility/department, a secured courier service or other delivery method that allows for positive tracking must be used.

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

3.4.11.1. 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).

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

3.4.11.3. Unsolicited email with credit card numbers must be printed out and immediately deleted.

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.

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

3.4.12.1. Processing sales and credits for our business only.

3.4.12.2. Never process a transaction for another business for any reason. If another business offers you the opportunity to process their transactions in exchange for money or a "cut" of the transaction, employees are to refuse and report the activity to management. Note that this is called "draft factoring" and is illegal and may carry penalties both for you and the business.

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

3.4.12.4. Settlement of transactions.

3.5. Paper Record Retention and Destruction

3.5.1. Records should be retained for no more than 2 years.

3.5.2. Orders may be destroyed immediately after the transaction is completed unless they are the only transaction record. In that case, they must be retained for 2 years. The PAN may be obliterated leaving no more than the last 4 digits of the card number to increase security.

3.5.3. All paper records containing credit card information must be clearly identified as Classified.

3.5.4. Records sent to long-term storage shall be shipped in a sealed and locked container and inventoried as to their location and destruction date. See Appendix B: Inventory of Storage Locations. All movements of records shall be logged.

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.

3.5.5. Records held for destruction shall be in locked, sealed containers and clearly marked "To Be Destroyed".

3.5.6. Destruction shall be performed securely by either an employee or a secure destruction service. Records held for destruction shall be clearly marked "To Be Destroyed" and stored in a sealed, locked container.

3.5.7. Destruction must be through shredding, incinerating or pulping.

3.6. Managers shall implement the following requirements:

3.6.1. Third party service providers must be contractually required to be PCI DSS compliant and to acknowledge responsibility for credit card information security.

3.6.1.1. Verification of third party PCI DSS compliance shall be by one of the following methods:

3.6.1.2. Ensuring the processing software is listed on PCI Security Standards Council's list of validated payment applications found at https://www.pcisecuritystandards.org/security_standards/vpa/ OR;

3.6.1.2.1. Ensuring third party providers are listed on Visa's list of approved payment applications found at http://www.visa.com/pabp OR;

3.6.1.2.2. Receipt of a vendor's PCI DSS compliance certification.

3.6.1.3. A list of third party providers shall be maintained.

3.6.1.4. Vendor PCI compliance shall be verified annually.

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.

3.6.2. Access to credit card information files shall be restricted to only those employees who need to use them as part of their job functions.

3.6.2.1. A list of authorized individuals shall be maintained in Appendix A.

3.6.3. This policy shall be reviewed annually and revised as needed.

3.6.4. Implementation of all policies shall be reviewed annually.

3.6.5. Appendix A to this policy shall be completed and updated as changes occur. The information is as follows:

3.6.5.1. Merchant Service Provider name and telephone number.

3.6.5.2. Manufacturer Name, Model Number and Serial number of all terminals.

3.6.6. Background checks shall be performed on all employees whose job functions allow access to credit card information files. This does not apply to employees, such as sales clerks, who only have access to one card at a time, however, they must attend Security Awareness training.

3.6.7. Each day verify the batch number for the start of the day is consecutive to the batch number from the previous day.

3.6.7.1. If not consecutive, contact customer service at the phone number on merchant service statement and follow their instructions immediately.

3.6.7.2. Notify the highest level of management immediately.

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.

3.7. In the event a credit card terminal is lost, stolen fraudulently used and/or you suspect theft of customer records:

3.7.1. Notify the Incident Response Team.

3.7.2. Incident Response Team members shall be listed in Appendix D.

3.7.2.1. Determine the extent of the breach.
3.7.2.2. Notify executive management.
3.7.2.3. Make required notifications according to local, state and federal laws and your merchant services contract.

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

3.7.2.4.1. Request that the Terminal ID (TID) be deactivated as soon as possible.
3.7.2.5. Incident response team members shall be documented in Appendix D. All employees shall be aware of the identity of the team leader (Chief Security Officer) and instructed to contact that individual if they suspect a breach or theft.

3.7.2.6. 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.

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

3.8. Training

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.

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

3.8.2. A record shall be maintained for each employee indicating the employee has read and understood each policy they are required to read. See Appendix C for form.

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

3.8.4. Training shall be documented in Appendix C.

4. References and Cites

4.1. PCI Data Security Standard v3.2

5. Records

5.1. Appendix A: Merchant Contact Information

5.2. Appendix B: Inventory of Storage Locations

5.3. Appendix C: Policy Training Record

5.4. Appendix D: Incident Response Team Contact List

Appendix A: Merchant Contact Information

Merchant Service Provider Name	Merchant ID Number	Customer Service Phone

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.

Credit Card Processing – IP Terminals
Version 3.2

Terminal Manufacturer	Model Number	Serial Number	Persons Authorized to use

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.

Credit Card Processing – IP Terminals
Version 3.2

Appendix B: Inventory of Storage Locations

Location – Address or Room	Storage Term (Circle One)	Destruction Date
	LONG/SHORT	
	LONG/SHORT	
	LONG/SHORT	
	LONG/SHORT	
	LONG/SHORT	
	LONG/SHORT	
	LONG/SHORT	
	LONG/SHORT	
	LONG/SHORT	

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.

Credit Card Processing – IP Terminals
Version 3.2

Appendix C: 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.

Credit Card Processing – IP Terminals
Version 3.2

Policy Appendix D: Incident Response Team Contact List

Name of Member	Role	Telephone Number
	Chief Security Officer	

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.