

**Credit Card Processing Security Policy
(as documented to meet PCI-Payment Card Industry Standards)**

Our business accepts credit cards as a form of payment. Controls for protecting cardholder data include the following:

- We use a credit card terminal that dials via the telephone for each approval. Neither the customer copy or the merchant copy of the receipt shows the entire credit card number - such truncation of the credit card number precludes others, such as customers, cleaning service, other staff that not is responsible for bookkeeping functions from having inappropriate access of cardholder data. We do not store any information that is on the magnetic strip of the card in any manner. At the end of each day, the printed batch report is balanced to day sheet activity for credit cards received. If there were any discrepancy in batch totals to individual posting activity, proper action would be taken to identify and resolve such discrepancies prior to entering deposit into accounting system. Monthly, credit card deposit activity is reconciled to bank statement and should there be any discrepancies, our credit card processor, Best Card (1-877-739-3952), would be contacted to determine missing activity.
- Should a customer call or mail in credit card number for payment on account, the credit card number and related information is properly destroyed immediately after processing payment. Credit card numbers are never sent via email and the internet is not used in any manner for receipt of payment. At no time are credit card numbers maintained in an unlocked manner in the office and no credit card numbers are stored on any computer records/files. All signed credit card receipts are kept at least six months for purposes of providing proper approval of the transaction should a chargeback from a customer be received. Credit card documents are never stored outside of the office and procedures require that all financial related records be shredded when destroyed.
- This policy is reviewed annually and personnel who are not responsible for accepting payments are aware of the sensitivity of protecting such data.
- Our service provider is Best Card (powered by First Data). Proper due diligence of our service provider was conducted (they are the endorsed program by my Association) prior to selecting them. Our service provider is responsible for maintaining proper security of cardholder data and they are responsible for maintaining proper controls to protect all data of our customers (via the payment process to deposit to my bank and offsetting charge to customer's account) in a secure manner.

Date(s) of policy review: _____

Staff responsible for oversight of credit card processing security: _____