Administrative Policy

1 Policy

1.1 This policy applies to all OPTIONS employees. The policy also pertains to all departments that process credit cards, including: transmitting or handling cardholder information. The cardholder information may be in a physical or an electronic format.

1.2 All transactions that OPTIONS processes must meet the standards outlined in the policy.

1.2.1 Electronic credit card numbers should not be transmitted or stored on a personal computer or e-mail account. Electronic lists of customer's credit card numbers should not be retained. Credit card information should only be accepted by telephone, mail, or in person. This information should not be accepted via e-mail and departments should not e-mail credit card information.

1.2.2 Physical cardholder data must be locked in a secure area. Access should be limited to individuals that require the use of the data. Access should also be restricted on a 'need to know' basis.

1.2.3 Only essential information should be stored. The Card Validation Code (also known as the Security Digits, V Code, or CID); users PINs or the full data from a cards magnetic strip are not to be stored.

1.2.4 Credit card information is to be retained for the time needed to process, or if retained for reconciliation, for a maximum of 3 months.

1.2.5 Credit card information, if it does not need to be retained, should be destroyed. Information should be destroyed by shredding immediately after processing, or immediately after it no longer needs to be retained.

1.2.6 Credit card receipts may only show the last four digits of the credit card number. If receipts show more than the last five digits, the receipts must be shredded or retained in a secure area.

1.2.7 Exceptions to the policy may be granted by the CEO or CFO.

1.2.8 External scans by an approved PCI scan vendor are required to be run on a regular basis.

1.2.9 Employees who handle credit card accounts are to be made aware of security policy and cardholder information practices upon hire and at least once a year thereafter.

1.2.10 Upon discovery of a cardholder information breach, OPTIONS will immediately contact NPC/Retriever Systems and First Data to report the incident.

1.2.11 The CFO has been designated as the Security Administrator has been assigned to ensure that the policy and security practices of OPTIONS are enforced and updated, as needed.

POLICY DATE:	March 2008
REVISED:	May 2012
REVISED:	April 2014
REVISED:	October 2015
REVIEWED:	October 2018
REVIEWED:	November 2019
REVISED:	November 2020