Estate Insurance Group Credit Card Security Policy September 2012

Introduction & Scope:

This document explains EIG's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. EIG's management is committed to these security policies to protect information utilized by EIG. All employees are required to adhere to the policies within this document.

Scope of Compliance:

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently EIG does not store cardholder data in an in electronic format, nor does it process or transmit any cardholder data on their systems or premises. Retention of cardholder data, if any shall be limited to paper reports or receipts.

Due to the limited nature of the 'in-scope' environment, this document is intended to meet the PCI requirements in Self-Assessment Questionnaire (SAQ) A, version 2.0, October 2010. Should EIG implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ, it will be the responsibility of EIG to determine the appropriate compliance criteria & implement additional policies and controls as needed.

Requirement: Restrict Access to Cardholder Data – Physically secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g. paper receipts, paper reports, faxes etc.) are subject to the following storage guidelines:

All media must be physically secured (PCI requirement 9.6)
Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include:
Media must be classified so the sensitivity of the data can be determined (PCI Requirement 9.7.1)
Media must be sent by a secure carrier or other delivery method that can be accurately tracked (PCI requirement 9.7.2)
Logs must be maintained to track all media that is moved from a secured area, and management approval be obtained prior to moving the media. (PCI requirement 9.8).
Strict control must be maintained over the storage and accessibility of media containing cardholder data (PCI requirement 9.9)

Destruction of Data:
All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)

Hardcopy media must be destroyed by shredding, incineration or pulping so that the cardholder data cannot be reconstructed. Container storing information waiting to be destroyed must be secured to prevent access to the contents. (PCI requirement 9.10.1)

Maintain a Policy that addresses Information Security for Employees & Contractors

EIG shall implement and maintain policies and procedures to manage service providers (PCI requirement 12.8)

Maintain a list of service providers (PCI Requirement 12.8.1)

Maintain a written agreement that includes an acknowledgment that the service providers are responsible for the security of the cardholder data the service provider's possesses (PCI requirement 12.8.2)

Implement a process to perform proper due diligence prior to engaging a service provider (PCI requirement 12.8.3)

Monitor service providers PCI DSS compliance Status (PCI 12.8.4)

Approved By Nick Sellick

Managing Director

September 2012