1.003 Payment Card Industry Data Security Standard (PCI-DSS) Policy

Policy Purpose and Scope

The purpose of this policy is to ensure departmental compliance with the Payment Card Industry Data Security Standard (PCI-DSS). This policy also makes all employees and persons associated with the Company aware of basic PCI-DSS practices.

Roles and Responsibilities

Each department for which this applies will be responsible for maintaining and enforcing its own specific PCI-DSS policy. The IT and Legal Department will be responsible for managing and implementing this overall Policy.

Operational Procedures

- ### Applicable Departments for Specific PCI-DSS Policies

  The Billing, Sales, and Client Services Departments each must establish, publish, maintain, and disseminate a PCI-DSS security policy compliant with the PCI-DSS.

- ### General Concept of PCI-DSS

  The Payment Card Industry Security Standards Council has instituted a standard for merchants (like PhotoBiz) to protect cardholder data. The PCI-DSS sets forth standards involving both technology hardware/applications and corporate behavior.

- ### No Receipt, Storage, or Dissemination of Cardholder Data

  Although your work may not typically involve the handling of cardholder data, there may be occasions where you will come into contact with cardholder data. Therefore, it is important for all associated persons to know that **PhotoBiz does not receive, record, or disseminate critical cardholder data** with limited exceptions. The first exception is when a sales, billing, or client services agent will verbally take cardholder data and directly enter it for payment (i.e. accepting a credit card payment over the phone). That data may not be written down or recorded in any form for any purpose. The second exception is that limited cardholder data associated with each account is kept for account verification purposes – namely: cardholder name, first four, last four, and the expiration date. No other cardholder data may be stored. Anyone violating this policy will be subject to discipline up to and including termination.

- ### Example

  You receive an email from a customer with their cardholder data. First, you should politely advise the customer in a separate email to not email cardholder data. Second, you should advise the IT department to make sure all traces of the cardholder is deleted.

Revision Date: December 2012