PCI Security Compliance Policy

Marion Public Library

The Marion Public Library abides by the following security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program.

I. SCOPE OF COMPLIANCE

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, the library's cardholder environment consists only of a single standalone dial-out terminal at the Check Out Desk. The library does not store cardholder data on any computer system.

II. PROTECTING CARDHOLDER DATA

A. The library does not store any authentication data, track or chip data, the card verification code, or the PIN under any circumstances.
B. Paper receipts are masked to show only the last four digits of the PAN (primary account number). Receipts are stored for four years, then shredded.
C. No cardholder data is transferred by any method except the designated standalone dial-out terminal at the Check Out Desk.
D. Access to the standalone dial-out terminal at the Check Out Desk is limited to library staff members who need to process patron payments.

III. SECURITY PRACTICES

A. This policy is reviewed annually and updated if necessary to reflect changes in relevant technology.
B. A security risk-assessment is conducted annually by the IT Coordinator.
C. Library staff is trained annually in the importance of cardholder data security ~~annually~~.
D. The standalone dial-out terminal at the Check Out Desk is inspected monthly for tampering ~~monthly~~ by the IT Coordinator.
E. In the event of a security incident, the Circulation and Access Services Manager will coordinate with the merchant bank, relevant credit card companies, and law enforcement.

Adopted by the Board of Trustees 4/13/2015

W1.1

Comment [CSS1]: PCI Requirement 3.2

Comment [CSS2]: PCI Requirement 3.3

Comment [CSS3]: Where? What about the reports we generate? Do those have any cardholder information? When we shred, we're supposed to keep a log.

Comment [CSS4]: PCI Requirement 9

Comment [CSS5]: PCI Requirement 4.2

Comment [CSS6]: PCI Requirement 7.1

Comment [CSS7]: PCI Requirement 12.1.1

Comment [CSS8]: PCI Requirement 12.2

We need to renew annually, and I'll review it all then.

Comment [CSS9]: PCI Requirement 12.6

Module in the Secure the Human training.

Comment [CSS10]: PCI Requirement 12.2

Added to my recurring to-do list.

Comment [CSS11]: PCI Requirement 12.5.3

Unless this should be me? Or Doug? I was thinking Jill actually works with it most.

Comment [CSS12]: Update with date when added to official policies.

Comment [CSS13]: Update when added to official policies.