**ASCLS-PA CREDIT CARD SECURITY POLICY**

**PURPOSE**

The purpose of this policy is to outline the security procedures employed when accepting credit card payments for educational meetings and other services in order to comply with the Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures.

**BACKGROUND**

Credit card payments are received by ASCLS-PA mostly for payment of registration for educational meetings. Credit card numbers are written by the attendees on registration forms and mailed to the registration chair for the meeting. The terminal used to process payments is a VeriFone, Inc. swipe terminal (Model Nurit 8320). Credit card numbers are entered manually into the terminal. This terminal is a standalone, dial-out terminal connected to a phone line.

**SECURITY POLICY**

1. Only the registration chair for the meeting who processes the payments has access to the credit card information submitted.
2. Registration forms submitted by attendees are maintained by the registration chair until the close of the meeting. This data is never in any area with public access. At that close of the meeting, the registration forms are shredded.
3. Credit card information is entered into a database. At the close of the meeting, this information is deleted from the program.
4. Reports generated from the program for payments sent to the treasurer have the credit card number obliterated to be unreadable before mailing to the treasurer. No identifiable credit card numbers are ever mailed or moved to any other location.
5. No data from the magnetic stripe on the back of the card are ever stored.
6. The three-digit security number from the back of the card (if provided by the payee) is never stored in the database or on reports to the treasurer.
7. No PIN numbers are ever collected from payees.
8. The printouts from the terminal have the PAN masked with only the last four digits displayed.
9. This security policy is distributed to the registration chair for the meeting who is the one who will receive the credit card information for processing. It will be maintained in the ASCLS-PA Handbook which is available on the organization website.
10. This policy is reviewed yearly to assure that it remains current with practices.
11. Any security breach of cardholder information will be reported to meeting attendees who paid by credit card.
12. ASCLS-PA does not have any service providers who receive credit card data.