**TO: ISM—{Chapter Name} Board and Officers**

**FROM:**

**SUBJECT: Payment Card Industry Data Security Standard (PCI) Compliance**

This document supersedes all previous PCI compliance policies and practices and is effective immediately.

ISM—{Chapter Name} and Institute for Supply Management® (ISM) considers data privacy to be critical and vital to protect our customers’, and members’ private information through the most effective methods we can reasonably employ.

1. **Purpose**

This policy specifically addresses payment card data; while most will not encounter payment card data during the course of their normal duties, all should be aware of what payment card data is and how to properly interact with and protect that data. This policy specifically covers the different types of payment card data employees may encounter and addresses the treatment of each type of data. It will also outline the minimum basic requirements for employees related to system security and maintenance to protect data.

1. **Personal Data**

Payment card data that is considered to be Personal Data includes:

* Payment card account numbers
* Cardholder name
* Payment card expiration dates
* Payment card service codes

Personal Data may be securely stored within one of our encrypted environments but cannot be retained on our non-encrypted environments (e.g. Fileshare, chapter computers, hardcopy (handwritten, printed or copied)), electronic storage devices or standard email systems). All customers should be advised that this information should be provided by phone or fax, but never via email, because we can’t ensure the security of emails in transit.

1. **Sensitive Authentication Data**

Information related to the following items is considered Sensitive Authentication Data and should never be stored, even within our encrypted environments:

* Full track data (data from a magnetic strip or chip)
* CAV2/CVC2/CVV2/CID (3 or 4-digit codes)
* PINs/PIN blocks

While we do not regularly require Sensitive Authorization Data, it is possible that someone could include it along with the Personal Data that is required. Sensitive Authentication Data should only be transmitted through phone conversations.

1. **System Security**

ISM—{Chapter Name} requires all users to have unique passwords that meet the following requirements:

* Contains both upper and lower-case letters
* Contains at least one number
* Is not an easily guessable password (i.e. “P@ssw0rd” or “I$M2021”)
* Is not in hardcopy form (handwritten, printed or copied) and stored in an insecure location

ISM—{Chapter Name} *understands in today’s environment people are required to utilize passwords for a wide variety of websites and programs. We highly recommend that users not reuse the same password(s) for multiple sites or programs.*

1. **Data Protection**

ISM—{Chapter Name} does not allow the storage of Sensitive Authentication Data in any form. Once the immediate need for the Sensitive Authentication data has passed that data must be destroyed. Sensitive Authentication Data should only be received over the phone. If this information is written down or printed the information must be destroyed immediately after the processing of the transaction(s). This information can never be stored for future use, even if there is an expectation of an order in the very near future or if there is a customer request to store the information.

Personal Data should be destroyed immediately after use. If the Personal Data is received via email, the email should either be deleted, or if the communication within the email (except for the Personal Data) needs to be retained the email should be redacted or edited and forwarded; then the forwarded email can be saved and the original email, with the Personal Data can be deleted. If the Personal Data is contained in an attachment that attachment can simply be removed within the email system.

ISM does not allow for any storage of Personal or Sensitive Authentication Data in hardcopy (handwritten, printed or copied) form. No payment card files should be created or maintained. Any files of this type that may be unknown at this time should be immediately destroyed as identified.

I have read, understand and acknowledge receipt of this policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(signature) (date)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(employee name)