

Denison accepts credit cards as payment for a variety of goods and services. By accepting credit cards, Denison assumes a level of risk with respect to a data breach. In order to manage that risk, credit card transactions processed at Denison will comply with the Payment Card Industry Data Security Standard (better known as PCI DSS.)

PCI DSS defined:

"The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data,"
(https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.)

By policy, Denison must be classified as PCI validation type four. Validation type four means Denison has one or more POS or payment systems connected to the Internet. In addition, there is no electronic storage of any card holder data (CHD). CHD at minimum is the primary account number (PAN) commonly known as the credit card number.

PAN Defined:

"Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account."
(https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf.)

Cardholder data may also appear in the form of the PAN plus any of the following including but not limited to cardholder name and expiration date.

(See https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_instr_guide.pdf)

Any Denison entity intending to process credit card transactions must adhere to the following terms and conditions:

1. Denison contracted vendors must be PCI compliant.
2. Electronic storage of the Primary Account Number (PAN) is NOT permitted under any condition within Denison's technology infrastructure:
 - 2.1. Including but not limited to:
 - 2.1.1. File servers,
 - 2.1.2. Desktop or laptop systems,
 - 2.1.3. Any other portable device,
 - 2.1.4. Tapes,
 - 2.1.5. External USB disk drives,
 - 2.1.6. USB pen or flash drives,
 - 2.1.7. DVD's,
 - 2.1.8. CD's,
 - 2.1.9. Any other media not named or known,
 - 2.1.10. Any personally owned hardware or media.
 - 2.2. In clear text, redacted, or encrypted
 - 2.3. Regardless of the length of time

- 2.3.1. There is no acceptable duration of time for storage of the PAN
- 2.4. Regardless of any firewall presence or configuration
- 2.5. Regardless of system ownership (e.g, third party systems are NOT exempt).
- 3. PANs, either in part or in full, may NOT be emailed under any circumstances.
- 4. PANs transmitted via the network:
 - 4.1. Must be encrypted at the source,
 - 4.1.1. Card swipe terminal,
 - 4.1.2. Browser,
 - 4.1.3. Any new source not yet known,
 - 4.2. Must remain encrypted during the entire transaction process.
 - 4.3. Must NOT return the PAN to Denison as part of the transaction.
- 5. Vendor solutions using a local host server or gateway within Denison's network, must be physically located in Fellows G1.
- 6. Transaction IDs *may* be stored for use as a transaction identifier. However, this ID must NOT include the PAN in part or in full.