PCI Data Retention and Disposal Policy

Policy Information

ISSUING OFFICE

Information Services

POLICY

Liberty University will protect cardholder data by using third-party credit card processing vendors in order to remove the necessity of storing any cardholder data (CHD).

STANDARDS

For Legacy System ONLY

Cardholder data storage should be kept to a minimum by implementing data retention and storage procedures that include at least the following:[1]

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Specific retention requirements for cardholder data
- Processes for secure deletion of data when no longer needed

Do not store sensitive authentication data (SAD) after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorized process.[2]

Render Personal Account Number (PAN) unreadable anywhere it is stored (including on any portable digital media, backup media, and in logs) by using any of the following approaches:[3]

- One-way hashes based on strong cryptography (hash must be the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures

Third-party processing

Mask PAN when displayed (last 4 digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the last 4 digits of the PAN.

Cardholder data should not be stored on any Information System.

If any cardholder data is discovered in any University Information System, it should be removed immediately by authorized personnel.

If an email is received that contains cardholder data, the cardholder data should be deleted and a response sent back to the sender, detailing how to proceed.

SCOPE

University personnel who handle credit card transactions, any other University personnel who discover stored CHD, and the personnel responsible to remove CHD, should it be found.

PURPOSE

Customer credit card details entrusted to the University must be afforded a combination of security measures (technological and procedural) which, in combination, prevent all recognized possibilities of the card details being accessed, stolen, modified, or in any other way divulged to unauthorized persons.[4] In an effort to protect cardholder data, Liberty University does not routinely store any credit card data on any system.

DEFINITIONS

CDE - ?Acronym for ?cardholder data environment.? The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.? (PCI Glossary, April 2018)

Information System - ?Discrete set of structured data resources organized for collection processing, maintenance, use, sharing, dissemination, or disposition of information.? (PCI Glossary, April 2018)

PAN - ?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.? (PCI Glossary, April 2018)

SAD - Acronym for ?sensitive authentication data?, which is defined as ?Securityrelated information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.? (PCI Glossary, April 2018)

Strong cryptography - ?Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is ?one way?; that is, not reversible). See Hashing.

At the time of publication, examples of industry-tested and accepted standards and algorithms include AES (128 bits and higher), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). See the current version of NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) for more guidance on cryptographic key strengths and algorithms.? (PCI Glossary, April 2018)

REFERENCES

ISO/IEC 27002:2013 (More information available upon request)

14.01.02 Securing applications services on public networks

18.02.04 Privacy and protection of personally identifiable information

PCI DSS 3.2

Requirement 3: Protect stored cardholder data

[1] . PCI DSS 3.1

[2] . PCI DSS 3.2

[3] . PCI DSS 3.4

[4] . ISO 14.01.02, 18.02.04 (ISO Policy 030805)