Data Storage Policy

Policy Information

ISSUING OFFICE

Information Services

POLICY

Data storage practices must ensure that data is readily available to authorized users and that archives are both created and accessible in case of need.[1] Information system media, both paper and digital should be protected (i.e., physically controlled and securely stored) [2]

STANDARDS

General

Cardholder data should never intentionally be stored on any information system media.[3]

Access to information system media is permitted only for authorized users.[4]

Media containing sensitive or highly sensitive data or information that is transported outside of controlled areas needs to be strictly monitored to control access and to form accountability.[5]

Approved cryptographic mechanisms or other alternative physical safeguards should be implemented to protect the confidentiality of information stored on digital media during transport.[6]

Approved cryptographic mechanisms or other alternative physical safeguards should be used during transmission in order to prevent unauthorized disclosure of information.[7]

Use approved cryptographic mechanisms to protect the confidentiality of sensitive and highly sensitive information at rest.[8]

Access to university information systems, equipment and the respective operating environments is limited to authorized individuals.[9]

Keys, locks, combinations, card readers, and other devices that allow entry into areas where sensitive or highly sensitive information is stored are to be controlled and monitored.[10]

Data Centers and Server Rooms

Protect and monitor the physical facility where data and information are stored and support infrastructure for those information systems.[11]

Any visitors to locations where data is housed will be escorted and their activity monitored.[12]

Audit logs will keep record of physical access to areas where data or information is stored or handled.[13]

Locations where data is stored, both on-site and remote, must provide access controls and protections in order to reduce the risk of loss or damage to an acceptable level.[14]

SCOPE

Any sensitive or highly sensitive data stored on Liberty University media

PURPOSE

The purpose of this policy is to provide guidance for properly handling Liberty University?s data and information. Most compromises of data privacy occur due to improper handling of data by trusted internal resources. Replaces previous policy PG0023.

DEFINITIONS

Cardholder Data (CHD) - For the purpose of this policy, CHD includes the primary account number (PAN) as well as any sensitive authentication data (SAN). Combined, these include, but are not limited to:

- Credit card number
- Card validation codes/values
- Full track data (from magnetic strip or equivalent in a chip)
- PINs
- PIN blocks

Data - A subset of information in an electronic format that allows it to be retrieved or transmitted.

Data at rest - Inactive data that is stored in any digital form

Cryptographic mechanism - Encryption tools used for protecting confidentiality, integrity, authenticity and non-repudiation of information.

Encryption - Process of converting information into an unintelligible form except to holders of a specific cryptographic key.

Information - Any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphical, narrative, or audiovisual.

Media - Anything containing private information entrusted to Liberty, including, but not limited to, FERPA data, HIPAA data, GDPR data, or PCI data

RELATED POLICIES

IS010108 Data Classification

IS020121 Acceptable Use Policy

REFERENCES

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

8.2.3 Handling of assets

11.1.2 Physical entry controls

11.1.3 Securing offices, rooms and facilities

18.2.3 Protection of documented information

NIST 800-171 More Information here

3.8 Media Protection

3.10 Physical Protection

3.13 System and Communication Protection

PCI DSS 3.2.1

Requirement 3: Protect stored cardholder data.

---

[1] . ISO 27000 8.2.3, 18.2.3 (ISO Policy 030502)

[2] . NIST 800-171 3.8.1

[3] . PCI DSS Requirement 3

[4] . NIST 800-171 3.8.2

[5] . NIST 800-171 3.8.5

[6] . NIST 800-171 3.8.6

[7] . NIST 800-171 3.13.8

[8] . NIST 800-171 3.13.16

[9] . NIST 800-171 3.10.1

[10] . NIST 800-171 3.10.5

[11] . NIST 800-171 3.10.2

[12] . NIST 800-171 3.10.3

[13] . NIST 800-171 3.10.4

[14] . I SO 27000 11.1.2, 11.1.3 (ISO Policies 090201, 090202)