Physical Security - Media Policy

Policy Information

ISSUING OFFICE

Information Services

POLICY

On-site locations where PCI data is stored must provide access controls and protection which will reduce the risk of loss or damage to an acceptable level.[1]

STANDARDS

Physically secure all media.[2]

- Store media backups in a secure location, preferably an off-site facility, such as an alternative or backup site, or a commercial storage facility. Review the location?s security at least annually.[3]

Maintain strict control over the internal or external distribution of any kind of media, by doing the following:[4]

- Classify media so the sensitivity of the data can be determined[5]
- Send the media by secured courier or other delivery method that can be accurately tracked[6]
- Ensure management approves of any and all media that is moved from a secured area (including when media is distributed to individuals)[7]

Maintain strict control over the storage and accessibility of media[8]

- Properly maintain inventory logs of all media and conduct media inventories at least annually[9]

Destroy media when it is no longer needed for business or legal reasons as follows:[10]

- Shred, incinerate, or pulp hard copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed[11]
- Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed[12]

Movement of hardware or any items within the PCI Inventory between the University?s locations is to be strictly controlled by authorized personnel.[13]

SCOPE

LU employees who handle PCI data; any media containing PCI data

PURPOSE

This policy should serve as a reminder to treat any PCI data in any location with the highest level of security reasonably possible. Many times, when the topic of the protection of data (in this case, PCI data) arises, the focus is generally on the access to the actual site where the data is stored or the level of access employees have within programs. It would be remiss to omit the actual storage areas in the direct control of employees who handle data every day. Items such as small pieces of paper, reports, and removable electronics media are often overlooked. The same level of security must be given to these seemingly insignificant items. Misplacing or wrong handling of any of these items when they contain PCI data could lead to adverse results and thus need to be protected.

DEFINITIONS

Media - For the purpose of this policy, media can be defined as including, but not limited to, computers, removable electronic media, paper receipts, paper reports and faxes.

RELATED POLICIES

IS010108 Data Classification

IS020107 Physical Security - Data Facilities

IS030502 Data Storage

IS030600 Backup Policy

IS030802 External Sharing

IS030805 PCI Data Retention and Disposal

IS050604 PCI Inventory

REFERENCES

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

11.01.02 Physical entry controls

11.01.03 Security offices, rooms, and facilities

PCI DSS 3.2: More information here

Requirement 9: Restrict physical access to cardholder data

---

[1] . ISO 11.01.02, 11.01.03 (ISO Policy 090201)

[2] . PCI DSS 9.5

[3] . PCI DSS 9.5.1

[4] . PCI DSS 9.6

[5] . PCI DSS 9.6.1

[6] .? PCI DSS 9.6.2

[7] . PCI DSS 9.6.3

[8] . PCI DSS 9.7

[9] . PCI DSS 9.7.1

[10] . PCI DSS 9.8

[11] . PCI DSS 9.8.1

[12] .?PCI DSS 9.8.2

[13] . ISO 8.02.03, 11.02.05 (ISO Policy 050405)