Media Destruction Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established a formal policy and supporting procedures concerning media destruction. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

The Office of Information Security will ensure that the Media Destruction policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Once the maximum retention period has been allotted for cardholder data, it must be removed from all electronic media, and any hardcopy edition must be disposed of accordingly.
- All hard copy materials are to be cross-shredded, incinerated or pulped, such that there is reasonable assurance the hard copy materials cannot be reconstructed.
- Storage containers for shredding hard copy materials are to be secured at all times, with appropriate physical controls such as locks on the storage bins.
- Storage of cardholder data on electronic media is not permissible per the PCI Compliance policy.
- All digital materials shall be destroyed when no longer needed.

Responsibility for Policy Maintenance

The Office of Information Security is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019