9. Sensitive Authentication Data (SAD) Storage Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Administrative Systems PCI Compliance Services has established a formal policy and supporting procedures regarding the storage of sensitive authentication data (SAD). This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Administrative Systems PCI Compliance Services' needs and goals.

Policy

Administrative Systems PCI Compliance Services will ensure that the storage of sensitive authentication data (SAD) is not allowed in any Stanford merchants system, and adheres to the following conditions for purposes of highly protecting card holder data and complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.0):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that sensitive authorization data is not stored after authorization in any Stanford merchant system.
- Sensitive authentication data includes:
    - Full track data (contents of any track from the magnetic stripe on the back of a card or equivalent data on a chip)
    - The three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data)
    - PINs/encrypted PIN blocks

Responsibility for Policy Maintenance

Administrative Systems PCI Compliance Services 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.