9. Sensitive Authentication Data (SAD) Storage Policy

Overview
In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, UIT-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 UIT-PCI Compliance Services' needs and goals.

Policy
UIT-PCI Compliance Services will ensure that the storage of sensitive authentication data (SAD) 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):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that 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) is not stored after authorization.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that PINs and encrypted PIN blocks are not stored after authorization.

Responsibility for Policy Maintenance
UIT 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.