VISA PIN SECURITY PROGRAM

PIN Security Program

Visa is committed to protecting the Visa payment system which includes Visa cardholder PIN data. To that end Visa created a PIN Security Program outlining compliance requirements with which acquirers, their merchants and/or their third party agents must comply. The baseline requirements for the Visa PIN Security Program include:

PCI PIN Security Requirements

The PCI PIN Security Requirements contain a complete set of controls for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.

The requirements include:

- Identifying minimum security requirements for PIN-based interchange transactions
- Outlining the minimum acceptable requirements for securing PINs and encryption keys
- Assisting all retail electronic payment system participants in establishing assurances that cardholder PINs will not be compromised.

They also include specific requirements for entities involved in the implementation of symmetric key distribution using asymmetric keys (remote key distribution), entities involved in the operation of Certification Authorities or perform key injection services.

Visa PIN Entry Device (PED) Requirements

The PED requirements help organizations protect themselves against PIN compromises, cardholder PIN data breaches, fraud, and ensures confidentiality and integrity of PIN data.

All Visa PIN Security Program Participants must deploy and use PEDs that are PCI PTS Approved and listed on the PCI Approved Device List.
https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

Also available is the Visa is the PIN Entry Device (PED) Requirements. These mandated requirements assist organizations in their PED purchasing, usage and deployment strategies, The Visa PED Requirements also identify actions required with a PED security approval expires.

Additional information on Visa PED Requirements are found in Appendix B of the Visa PIN Security Program Guide.

Visa TDES Requirements

Visa's Triple Data Encryption Standard (TDES) requirements are:

- All ATMs must use TDES to protect pins
- All POS PIN acceptance devices must use TDES to protect pins.

U.S. only: Automated fuel dispensers (AFDs) must use TDES or Single DES Derived Unique Key per transaction (SDES DUKPT) to protect PINs. Sunset date for SDES DUKPT is 1 October 2020.

Adherence to the requirements of the Visa PIN Security Program results in more than simply securing PIN data. Sound security practices help to protect organizations from adverse financial and reputational consequences often associated with PIN data compromises.

PIN Security Program Participants

Validating Participants

Organizations identified as Validating Participants must validate to Visa their compliance with the requirements outlined in the Visa PIN Security Program Guide. Validation is required every 24 months using a Visa Approved PIN Security Assessor.

Validating Participants are defined as:

- **PIN Acquiring Third-Party VisaNet Processor (VNP)** – A third party VNP entity that is directly connected to VisaNet and provides acquiring PIN processing services to Visa clients
- **PIN Acquiring Client VNP acting as a Service Provider** – A Visa client or client-owned entity that is directly connected to VisaNet and provides PIN acquiring processing services to Visa clients
- **PIN Acquiring Third-Party Servicers (TPS)** – A third-party agent that stores, processes, or transmits Visa account numbers and PINs on behalf of Visa clients
- **Encryption and Support Organizations (ESO)** – Organizations that:
    - Perform cryptographic key management services (i.e., key injection facilities (KIFs), Remote Key Injection (RKD) on behalf of Visa clients
    - Service and/or deploy client ATM, POS, or kiosk PIN entry devices (PEDs) which process and accept cardholder PINs
    - PED manufacturers and third party Certificate Authorities that manage various cryptographic key management responsibilities for clients

Non-Validating Participants

Visa clients, merchants and other organizations that are not identified as Validating PIN Participants must perform appropriate due diligence to ensure compliance with the Visa PIN Security Program requirements. This may include performing self-assessments using an internal or external resource. Individuals performing the self-assessment must have adequate knowledge of the PCI PIN Security Requirements but do not need to be Visa Approved PIN SAs.

Self-assessment results do not need to be submitted to Visa, however Visa may request evidence of PIN security compliance or request an on-site PIN Security review of any organization, at any time, to ensure the security of the payment system.

Visa reserves the right to re-categorize Non-Validating Participants as Validating Participants that must demonstrate compliance according to requirements outlined in this Visa PIN Security Program Guide.

Refer to the Visa PIN Security Program Guide for the full set of requirements for Validating and Non-Validating PIN Participants.

For More Information

For more information about the Visa PIN Security Program, contact your regional Visa program manager:

AP and CEMEA:	pinsec@visa.com
Europe:	visaeuropepin@visa.com
LAC:	pinlac@visa.com
North America:	pinna@visa.com
Global:	pin@visa.com