What Are the PCI PIN Security Requirements?

33 requirements across 7 control objectives, designed to protect PINs, cryptographic keys, and the systems that process them.

01 PIN Security

- Protect PINs during capture, processing, and transmission
- Prevent unauthorized disclosure of PIN data
- Use approved PIN encryption techniques
- Protect PIN blocks from compromise

02 Cryptographic Keys

- Generate keys using approved methods
- Protect keys from unauthorized disclosure
- Control key usage and cryptographic functions
- Secure keys throughout their lifecycle

03 Key Management

- Apply dual control
- Maintain split knowledge
- Secure key distribution and loading
- Control key rotation, replacement, and destruction
- Maintain key-management records

04 Cryptographic Devices

- Secure Hardware Security Modules (HSMs)
- Restrict access to cryptographic functions
- Maintain secure device configurations
- Protect cryptographic equipment from tampering

05 Physical Security

- Restrict physical access to sensitive equipment
- Protect key components and cryptographic materials
- Secure key-loading and key-management areas
- Detect and respond to physical tampering

06 Logical Security

- Enforce strong authentication and access controls
- Restrict privileged access
- Separate security-sensitive functions
- Monitor and log access to critical systems

07 Operational Security

- Establish documented security procedures
- Define roles and responsibilities
- Maintain audit trails and monitoring
- Regularly review security controls
- Manage security incidents and exceptions

www.ampcuscyber.com | letsconnect@ampcuscyber.com