UNIVERSITY OF OKLAHOMA
Campus Payment Card Security
Supplemental Requirements for Merchant Mobile Devices and Networks
Norman Campus

Note: This document contains a list of requirements. Business Units/Merchants must comply with the below and any other requirements of the PCI Steering Committee. Business Units/Merchants must obtain either a separate agreement/MOU signed by the appropriate department head, or an addendum to the respect merchant's Office of the Bursar's Merchant's Contract, which includes the Business Unit/Merchant's acceptance of these requirements as a prerequisite for consideration by the PCI Steering Committee to permit the use of mobile devices in the cardholder data environment.

Requirements:

Business Units/Merchants seeking to implement or support mobile devices or networks in any of the following capacities may do so only when consistent and compliant with special supplemental requirements established by the PCI Steering Committee for merchant use and support of such mobile devices and networks:

- Use of mobile devices and networks for merchant payment acceptance, processing, or storage.
- Use of mobile devices within the Cardholder Data Environment (CDE) and use of mobile networks of the CDE for purposes other than payment acceptance, processing, or storage.
- Merchant support for consumer-side uses of mobile devices outside the CDE, including payment-initiation applications and technology.

Compliance with existing policy and standards:

- Existing requirements for merchants to notify and obtain prior approval by the Office of the Bursar for any changes to existing environments, technologies and/or processes associated with the CDE remain applicable to any and all changes involving mobile devices.
- Business units storing, processing or transmitting cardholder data must comply with all relevant aspects of the most current PCI DSS requirements and procedures within the allotted grace period set forth by the Payment Card Industry Security Standards Council ("PCI SSC") as well as follow all established University and Business Unit security standards and procedures for the Cardholder Data Environment.

Supplemental Requirements:

In addition to any and all other requirements established by the PCI Steering Committee, merchants seeking to use or support mobile devices in any of these capacities must ensure the following standards have been met, validated, and maintained:

Compliance with Applicable PCI SSC Guidance for Mobile Payment Acceptance

- All mobile device solutions must be implemented in accordance with the current version of the PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users.
- All custom mobile device solutions must be developed in accordance with the PCI Mobile Payment Acceptance Security Guidelines for Developers.

Management of Risks of Mobile Device Solution

- A merchant seeking approval of the implementation of a mobile device solution must perform and provide evidence of performing due diligence in the identification, selection, implementation, and operation of the solution, including the genuine management of risk, including risk assessment, risk response, risk communication, and risk authorization.

Tokenization and Point to Point Encryption for Payment Transactions

- Solutions involving mobile devices in the CDE must implement a robust method of removing the PAN to limit scope of the CDE (e.g., tokenization) and replacing it with a secure surrogate token.

- Any solution retrofitting a legacy system to achieve this functionality must ensure that existing PAN data is similarly abstracted from (tokenized) *and* removed from the POS software and the CDE.
- Any mobile solution must properly implement a point to point encryption (P2PE) solution using both hardware-encryption and certificate authentication directly to the acquiring bank, whether operating over merchant/University networks or public/untrusted networks.
- For any implementation of P2PE, either a third-party managed P2PE solution or a University/merchant-managed P2PE solution may be used. Where possible, a PCI SSC validated P2PE solution is strongly preferred.
- The PCI Steering Committee does not specify a single technology, implementation, or standard to accomplish this. The tokenization programs offered from acquiring banks, such as First Data TransArmor or MerchantWare Transport, are acceptable, where OU has a relationship with the acquirer and risks related to the implementation of the solution have been assessed and managed.

Single-Purpose Devices and Device Ownership

- Mobile devices used for, or supporting merchant mobile solutions used for, merchant payment acceptance, processing, or storage must be dedicated, single-purpose devices. Such devices cannot under any circumstances be used for any other purpose than the point of sale payment acceptance, processing, or storage application.
- Mobile devices must implement application whitelisting, enforcing restrictions on the use of the device to specific pre-defined applications and functions. Solutions that require web browser functionality must implement URL whitelisting to limit use to specific designated resources.
- Mobile devices used for, or supporting merchant mobile solutions used for, merchant payment acceptance, processing, or storage must either be owned and managed by the University or owned and managed by a third-party provider that is approved by either the PCI SSC or by the acquiring bank for the respective merchant transactions.

Active Mobile Device Policy Management and Enforcement

- Merchant must develop administrative and technical policies for mobile device and mobile application security and for mobile device account management.
- All mobile devices in the CDE must have security policies enforced, and those policies must be managed, monitored and reviewed by IT staff in compliance with industry security best practices and PCI standards.
- Mobile devices must be configured according to standards derived from and mapped to the current security benchmark or baseline provided by the Center for Internet Security for the respective platform.
- Mobile devices and their management systems must be configured to
    - Detect and alert on mobile devices that have been "rooted", "jailbroken", or similarly modified to attain root privilege control, to bypass the authorized bootloader, or to sideload unsigned applications/overcome protections of secure sandbox environment for applications.
    - Identify and track device location.
    - Support the secure remote wipe of the device on-demand by authorized administrators.

Physical Security

- Merchants must incorporate physical security of mobile devices into their personnel policies and operating procedures for the proper use, identification, storage, location and handling of the device.
- Employees are to be personally responsible and accountable for the use of mobile devices given to their care and control.
- All mobile payment devices must be stored in a physically secure cabinet, safe, or other enclosure until checked out and removed by an authorized employee.
- Employees must maintain, exercise, and assert diligent control over mobile devices.
- Mobile devices should be marked in a way that clearly differentiates them from other like devices and makes them immediately visible and recognizable (e.g., such as by a distinct cover or case).

- Mobile devices should have automatic proximity boundaries applied to their physical location (such as via use of RFID scanners on store exits, geofencing, and enforced automatic wipe when proximity connectivity loss limits are exceeded).

Mobile Networks

- Any wireless network for a permanent or semi-permanent storefront or point of sale location using 802.11 Wi-Fi or 802.15 Bluetooth technologies must be implemented in accordance with the current version of the PCI Data Security Standard (PCI DSS) Information Supplement: PCI DSS Wireless Guidelines.
- In addition to the network logging and monitoring requirements of the PCI DSS, mobile device networks used for merchant payment acceptance, processing, or storage must implement:
  - Connection logging for all traffic allowed or denied through the firewall isolating the mobile device network.
  - Flow-based network logging for all traffic flows [within the mobile network and] between the mobile network and the CDE.
  - Active monitoring and review of network flow and log data for anomalies, attacks and outages.