Security standard for merchant payment card processing

**Issue Date:**
The Security standard for merchant payment card processing was issued on July 30, 2019.

**Effective Date:**
The Security standard for merchant payment card processing is effective as of July 30, 2019.

**Purpose:**
Kennesaw State University (KSU) is committed to maintaining the security of customer information, including payment cardholder information such as payment card account number, payment cardholder name, expiration date, and payment cardholder verification number. In order to facilitate secure business operations, KSU follows the best practices for protecting payment card information as defined by the Payment Card Industry Security Standards Council. All Payment Card Processing at KSU must adhere to these standards to ensure institutional compliance with payment card handling and help ensure the security of customer information.

**Scope:**
The Security Standard for Merchant payment card processing impacts all KSU computers, payment terminals and other electronic devices involved in processing payment card information. PCI compliance is required of all eCommerce merchants that store, process or transmit credit cards, use equipment with external facing IP addresses, and all other payment channels including manual processing techniques such as, but not limited to, point-of-sale terminals and cash registers.

**Standard:**
University Information Technology Services and The Office of Fiscal Services require the following actions be taken:
1. All Merchant accounts must be obtained through, and registered, with the KSU Office of Fiscal Services

2. All Merchants must utilize the KSU contracted payment processing services. In the event that the university contracts with a 3rd party which includes payment processing services, the requesting department/college remains responsible for ensuring the contracted 3rd party provides proof of continued compliance annually to KSU UITS.

3. Point to Point Encryption (P2PE) is the required method for the accepting of payments when utilizing the university network. If the merchant solution is not P2PE certified, it must be removed from the university network and another method for connectivity used, such as cellular or analog phone line.

4. If utilizing the central processing services, merchants shall not transmit or store cardholder data outside the centralized system.

5. All systems processing payment card information must comply with applicable PCI Standards regarding change management, device configurations, and secure handling processes.

6. Only one primary function (e.g. – web, database, or application server) is allowed per server and the university unit must maintain a list of all devices associated with payment card processing. Additionally, remote access must be managed in alignment with PCI requirements.

7. All applications processing payment card information must have been procured via approved university purchasing processes and be registered with the Office of Fiscal Services as stated above.

8. All payment card business and data handling processes must comply with applicable university policies including (but not limited to) the Computer Usage Policy, Data Security Policy and New Server Policy.

9. All merchants and credit card service providers MUST annually complete, and provide a copy to KSU, a PCI-accepted Attestation of Compliance (AoC). All responses shall be coordinated with the UITS Office of Cybersecurity.

10. All systems processing payment card information must use fixed IP addresses, or use a documented dynamic range, on an isolated network. Access to these systems should be configured in alignment with PCI configuration requirements.

11. Using any wireless connectivity for payment card processing is not authorized unless it is a validated component of the approved merchant solution.
12. All web servers providing payment card processing services must utilize the strongest transmission encryption possible and hand the processing off to a 3rd party processor via a tokenization or PCI-compliant encryption process.

13. All portable devices processing payment card information (laptops, handheld scanners, etc.) and any desktops located in physically insecure environments must implement encryption (full-disk or device).

14. All physical media and devices associated with payment card processing must be maintained throughout the device and media lifecycle, including distribution, accessibility, and surplus.

**Review Schedule:**

The Security standard for merchant payment card processing will be reviewed annually by the Office of Chief Information Officer and the Office of the Chief Business Officer, or their designee.