830.11- Electronic Financial Transactions/Mobile Online Payment Applications

Purpose:

To ensure BSC maintains compliance with The Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

Procedure:

Mobile Online Payment (MOP) Application Definition:
MOP applications are special applications that are downloaded for use on electronic mobile devices like iPads, tablets, and laptops and are used to process credit card payments.

MOP Software Applications:
- MOP Software for payments must be approved by BSC Information Technology Solutions and Services, Bank of North Dakota, and BSC Student Finance.
- Merchant numbers for payment processing must be obtained through BSC Student Finance.
- The application must require authentication and authorization (e.g., login and password).
- The application must have the capability to purge transaction data after the required 90-day period when a charge can be disputed by the customer.
- SSL certificates are required and must be up to date.

Using the Right Devices:

1. The device and associated hardware must be assigned to a specific, full-time, benefitted employees can use these apps, and they must use BSC-owned devices. This person is responsible to ensure that all requirements, standards, and guidelines are met.
2. A list of wireless devices used for payment processing, along with who has authorized use must be maintained by the department and devices must be registered with the Director of Student Financial Services.
3. The device must be a BSC-owned device with software used solely for the purpose of processing payments. Only the payment application and the operating system software are allowed on the device.
4. Devices are limited to wireless connections which are secure.
5. No personal phones, laptops, tablets, iPads, notepads can be used.
6. The device must be password-protected.
7. The device must have encryption capabilities.
8. Bluetooth capabilities must be turned off or disabled.
9. Automatic search and connect to external wireless networks must be turned off or disabled.
10. The device used for wireless electronic credit card processing must only be used by those who have a need to use and are authorized by the owning department/college and have data confidentiality and PCI training.
11. The use of a card-reader (if available) with the application is optional. The card-reader must also be approved by BSC Student Finance and Bank of North Dakota.

**Keeping Things Safe When Not in Use:**

- When the device is not processing payments, it **must** be turned off and stored in a safe place, like a locked drawer, file cabinet, or vault.

**References:**

[Gramm Leach Bliley Act, Payment Card Industry Data Security Standards (PCI DSS), NDUS 1203.7 Data Classification and IT Security Standard, SBHE 802.7 Identity Theft Prevention](#)

**History of This Procedure:**

First procedure: October 23, 2013
Approved by Executive Council on October 30, 2013; October 21, 2016.

Changed to Operational Procedure and approved by Doug Jensen on October 13, 2023.