PCI Compliance - Required Procedures for Faculty and Staff (**Secure login required***)**

Payment Card Procedural Requirements: GENERAL

1. All payment card processing is subject to review by the Payment Card Oversight (PCO) Committee to help ensure the College at Brockport's compliance with Payment Card Industry (PCI) standards.
2. No cardholder information is to be stored electronically on any device. Delete any pre-existing cardholder information from electronic databases, including computer hard drives, CDs, disks, and other external storage media. Contact LITS Help Desk at https://suny.service-now.com/ (585-395-5151 Option 1) for assistance coordinating the destruction of electronic media containing cardholder data.
3. In order for any department to store cardholder information, the rationale must be documented by the department and submitted for approval to the Payment Card Oversight Committee.
4. Sensitive authentication data (e.g.,CVC2, CVV2, PIN) may not be stored under any circumstance.
5. Paper documents containing cardholder information must be treated as confidential and secured properly (i.e., locked in a secure location) at all times.
6. Documents containing cardholder information must be destroyed using a micro-cut or cross-cut shredder after payment transaction authorization has been received. The payment transaction authorization code should be retained according to the College's Records Retention guidelines. See http://www.brockport.edu/accounting/recordsretention.html for specific information.
7. Inventories of paper documents containing cardholder information must be conducted by the appropriate department on at least a quarterly basis to ensure secure destruction of stored data that meets or exceeds defined retention requirements.
8. Access to cardholder information must be limited to those individuals whose job requires access.
9. College at Brockport employees, including student workers, who handle cardholder information must receive training on at least an annual basis, and must acknowledge their understanding of their responsibility for compliance with College policies and procedures.
10. Staff may not direct students/customers to a specific computer to make an online payment
11. Third-party vendors utilized by the College must provide evidence of annual PCI compliance both prior to entering into a contract, and on an annual basis thereafter.
12. Background checks must be performed on each employee, including student workers, who will be handling cardholder information.
13. Suspected security incidents must be reported immediately.
14. Payment card transactions must represent bona fide purchases of goods or services between the College at Brockport and the cardholder.
15. Cardholder information may not be sent or accepted via unencrypted electronic communication (e.g., email, instant messaging, chat, text messaging).
16. Refunds of credit card payments should not be given in the form of cash, check, or in-store credit. Refunds should be processed to the card used in the original transaction.
17. Refunds may not be issued for more than the amount of the original payment card transaction