Prohibited Practices:

- Storing CVV codes, pin numbers or track data and not destroying it immediately after processing.
- Sending credit card information via end-user messaging technologies (i.e. email, fax or intercampus mail).
- Instructing customer to send credit card information through the US Mail (without a dedicated PO Box or Lockbox) or via end-user messaging technologies (i.e. email, fax, or intercampus mail).
- Directly passing credit card fees to customers who pay via credit cards and charge lower amounts to customers paying in another manner. You may however, raise the rates across the board, regardless of payment method to offset fees.
- Using non-designated PCI compliant shredding devices or services.
- Using non-designated PCI compliant hardware to process credit card transactions.
- Using Square©, other swipe devices or apps without prior approval. Mobile devices or apps are not PCI compliant.
- Recording credit card information (call in transactions or automated voice transactions).
- Do not repeat a credit card number while over the phone in case others can listen in. Ask the caller to repeat the card number for your verification.
- Using non-approved third party service providers to process credit card transactions.
- Storing credit cards left behind for extended period of time, refer to Credit Card Left Behind procedures on PCI website.
- Mailing or transporting credit cards left behind to customer. Customer MUST pick card up at facility it was left or card must be destroyed.

Accepted Processing Procedures:

- Approved Secure Website (GVSU Hosted Order Page) - web solution handled by Institutional Marketing using Cybersource, contact Dave Poortvliet.
- Approved Secure terminal – wired or wireless, must be purchased through the Business & Finance Office.
- Call-in/low volume option taken directly to cashier window on same business day by GVSU employee (non-student) or call the Student Accounts Office immediately at EXT 12209 to make a “departmental credit card deposit” (provide FOAP before transferring call) or call 16050 for gift deposits.
- Dedicated PO Box for U.S. Mail or Wholesale Lockbox See below for additional details on these options.
- Approved PCI compliant vendors.
- Note: if using or considering a third party service provider to accept credit cards, the vendor must be PCI compliant. Notify the Associate Vice President & Chief Information Officer of
process to allow for proper documentation to be acquired from third party vendor before proceeding.

- Designated PCI compliant computers and other technologies (wireless access prohibited via this policy unless noted below), all other computers and technologies are PROHIBITED from accepting credit card information, contact the Associate Vice President & Chief Information Officer with questions. PCI compliant hardware can only be used in designated areas that are covered by the PCI network environment.

- Designated Vendor approved devices are allowed, all other devices are PROHIBITED from accepting credit card information, contact the Associate Vice President & Chief Information Officer with questions.

**GVSU and Vendor Application Passwords**
It is prohibited to store any GVSU or vendor application passwords in a non-secure environment. The risk from hackers using malware, phishing, or spear-phishing has changed our requirements for password storage:

Do Not Store Passwords in:
- Email
- Personal N: drive
- Hard drive
- Phone

Accepted Password storage locations:
- On paper in locked drawer
- Departmental L: drive with limited access and file password protected
- Password Manager tool on network drive (request instructions from IT)
Additional Detail on receiving CC payments via PO Box and Wholesale Lockbox

PO Box
- Each department that receives CC data via US Mail must acquire their own PO Box. When setting up a new PO Box, be certain to provide the department name and address to distinguish from other GVSU departments with PO boxes.
- Have mail delivered via USPS to specific office or have department pick up with secure process by GVSU non-student employee.
- Secure Process for pick up.
- Full Time staff who have been trained in PCI compliance allowed to pick up mail out of PO box.
- Special, *tamper evident bag to transport mail containing CC information. Contact the Business & Finance office to discuss options.
- Secure area where CC info is stored after received
  - Locked office/desk/drawer.
  - Install camera if storing CC info, if processing immediately upon receiving, no need for a camera.
  - If data does not need to be stored, shred data immediately after processing.
  - If data needs to be stored, store in locked cabinet or drawer (all CVV, track data and PIN#'s must be destroyed immediately and not stored) and define the length of time data is stored. Destroy data based on the storage policy guidelines within the Security Policy, see sections 4.2, 4.3, 4.4.
  - Process data within secured area.

Wholesale Lockbox
- Fifth Third Bank service to process CC data directly.
- Contact the Business & Finance Office for costs and set up.

All Other Accepted Methods of receiving CC payments (Drop In/Events/Phone Calls/Recurring Payments)

Option 1 - Handle CC data immediately via approved PCI compliant devices
- Dip/Insert/Swipe card if possible.
- If hand entered, put in all information requested – address, zip, cvv.
- Have customer sign the merchant copy of the receipt. (Name will appear if not hand entered; can also use the merchant copy to make notes on detail of the sale if needed).
- Offer customer their own copy of the receipt.
- Save merchant copies for settlement at the end of the day.
- Run the settlement process each night. This is what gets the money to the bank and puts the charge on the customer account.
- Complete a daily cash report through OnBase for each separate settlement. This is what gets the money into the proper Banner FOAP.
- Keep settlement report & merchant receipts for 7 years.
- If the machine has not been used frequently, test using a pcard or personal card. You can also run through a credit.
- If you test a settlement, you should still send a daily cash report through OnBase.
- Terminal support: First and best line of defense is the terminal helpline. Phone number is on the side of the terminal. You will be asked to provide the merchant ID, your name, and the department/address of the merchant (provide what shows up on the printed receipts).

**Option 2 - Process transaction immediately via manual process:**

- Credit card information called in to a department can be written down by a staff member as long as it is taken directly to a cashier window by the end of the current business day by a GVSU employee (non-student). The credit card information should be appropriately secured (stored and labeled) between the time it is written down and it is taken to the cashier window.
- If it cannot be taken to the cashier window by the end of the current business day, it should be called in to Student Accounts hotline (X12209 and provide the FOAP before transferring the call) or call 16050 for gift deposits.
- The name on the card and last four digits can be included in the top half of the departmental deposit form and can be saved by the department for record keeping purposes.
- The full credit card number and expiration date should be written on the bottom section of a departmental deposit form. This part should be detached and shredded by the cashier upon completion of the transaction. Credit card numbers, expiration date, and CVV data must never be stored by the department. This information may be requested as long as it is processed immediately and never stored.

**Option 3 - Process transaction at a later point in time, not current business day**

- Secure area where CC info is stored (secured and labeled) after received and until processed
  - Locked office/desk/drawer
  - Install camera on secure storage area
  - Process transactions next day or as soon as possible via methods discussed above
  - If data does not need to be stored, shred data immediately after processing
  - If data needs to be stored, store in locked cabinet or drawer (all CVV, track data and PIN#'s must be destroyed immediately and not stored) and define the length of time data is stored. Destroy data based on the storage policy guidelines within the Security Policy, see sections 4.2, 4.3, 4.4.
  - Process data within secure area
Laptop Use
- Any laptop that has access to CC processes must require encrypted hard drive
- VPN access required, no wireless access
- Logging of all transactions on laptop
- 2 Factor authentication
- Firewall
- Same environment that we are setting up for any PC in scope

Video Camera Options
- Contact the Associate Vice President & CIO for information.

Shredding Requirements
- Contact the Business & Finance Office for approved shredding options.
- Purchase individual shredder with diamond or cross cut technology
- Departmental contract secure drop areas which are shredded by outside vendor

Information Security Policies and Procedures for Cardholder Data

- Employees who process credit card data
  - Will be informed of Payment Card Industry (PCI) requirements by the PCI Committee on an annual basis.
  - Will be requested electronically to sign off that they have read the PCI Security Policy document on an annual basis.
  - Will be requested to electronically sign off on GVSU PCI Processing procedures on an annual basis.
- NOTE: All suspected security breach incidents should immediately be brought to the attention of the Associate Vice President & Chief Information Officer or any other member of the senior IT management for investigation. Contact the Office of Information Technology at 616-331-2035.
- GVSU PCI review of all Service Providers will be conducted annually by the Associate Vice President & Chief Information Officer to ensure PCI compliance is up to date for any vendor we are doing cardholder data business

All visitors in the in-scope areas will:

- be accompanied by an employee at all times
- be issued a VISITOR badge
- be signed into a log sheet with date/time stamp in and out