Best Practices for Payment Card Activities

Understand the Required Policies and Procedures

Make sure you are familiar with Virginia Tech's PCI policy, (contained in Policy No. 3610) and the Bursar's Office website for important payment card industry information. Compliance with the PCI standards at www.pcisecuritystandards.org is mandatory.

Protect Cardholder Data

- In order to mitigate some of the risk of accepting credit cards as a method of payment, departments should consider using Commerce Manager when practical.
- Do not request or send any credit card information by e-mail. If someone emails their information to you, you should first redact the card information and let them know that for their own safety you are not able to process the transaction via email. Ensure you delete their email to you as soon as possible to remove the cardholder information from your email.
- Departments must scan computers to ensure that the CHD is not stored unintentionally. It is recommended that department procedures require Identify Finder to run at least monthly to ensure that credit card data is not stored on the department's computers or employee's email accounts.
- Departments must ensure that all computers handling credit card data possess the most recent updated versions of university recommended antivirus and spyware detection software. Virginia Tech provides free antivirus software which can be downloaded at www.antivirus.vt.edu.
- Never use vendor supplied default passwords.

Implement Strong Access Control Measures

- Ensure that anyone who wants to set up a merchant account goes through the proper channels within your department prior to contacting the Bursar's Office.
- Make sure a background check is performed for all employees (both current and new) who will access or handle cardholder data.
- Each employee who has access to payment card information via computer should have a unique log-in or password. Employees cannot share passwords or log-in information.

Restrict Physical Access to Cardholder Data

- Departments should maintain all card acceptance equipment and documentation in a secure environment limited to accountable staff with a documented need to acquire access. Secure environments include: locked drawers, locked filing cabinets in a locked office and safes. Physical space can also be secured by the use of employee badges, swipe card/key access and

video camera monitoring of certain areas (i.e. customer service area, cashier/teller area and card documentation storage area).

- Ensure that the area used to process card payments is restricted to authorized employees and that any guests are authorized before entering the card processing area. Card data should not be in plain sight when guests or visitors are allowed into the office or card processing area(s).
- Crossing through the primary account number (PAN) and card data is not an acceptable means of securing the data on paper. Instead, cut off or remove that piece of the form for shredding.
- Shred any paper containing credit card numbers immediately following processing as you only need the transaction ID to handle disputes or credits/refunds. Cardholder data must be shredded using a cross-cut shredder.

Best Practices for a "Card Present" Transaction

- Swipe and retain the card until the transaction is authorized. This ensures that the card does not come back unauthorized subsequent to returning the card to the client.
- Give the customer their receipt to sign, if applicable. For "card present" transactions using a VISA debit card, merchants may not require a signature for purchases under $25.
- Compare the signature on the receipt to the one on the card.
- Do not accept cards saying "see ID." Have them sign the card and compare it to their driver's license or ask for another form of payment.
- The university does not recommend accepting unsigned cards. If a department chooses to do so, the department accepts all risk for those transactions. Departments accepting unsigned cards must require a second form of signed, picture ID prior to completing the transaction.

Best Practices for a "Card Not Present" Transaction

- Direct cardholder to complete transaction through the department's online payment system.
- Do not offer to enter payment card data into a third party website on behalf of a customer. The act of entering a payment on another's behalf could expose your computer and every computer connected to it. Instead, direct customers to access any internet enabled computer to complete their transaction.
- If your department accepts credit cards through a paper form (i.e. mail), we recommend that you structure the form so that the credit card data can be removed (i.e. perforation at bottom of page) and shredded immediately following processing. This allows for the other information to be retained for business purposes without restriction since the cardholder data is removed.
- If card data is accepted by phone, develop a standard form, preferably on color paper, that is easily identified as containing card data and which can be shredded after the transaction is authorized (see above).
- Follow acquirer's recommendations regarding the acquisition of CVV, AVS, etc., to identify potentially fraudulent activities and reduce the risk of chargebacks in "card not present" transactions.

- Use good judgment on first time shoppers, urgent or overseas deliveries, and large purchases made with several credit cards and shipped to the same address.