Viterbo University
Credit Card Processing & Data Security Procedures and Policy

The requirements for PCI-DSS compliance are quite numerous and at times extremely complicated due to their interdependent nature and scope. The University has deemed it necessary for those areas currently taking credit cards or debit cards to become familiar with and to implement acceptable practices that are compliant with PCI-DSS regulations. The intent of this document is to present the simplest and clearest picture of what is and what is not acceptable regarding credit card handling procedures and data security. Compliance is mandatory.

<u>Vocabulary</u>

Cardholder Data: Cardholder data is any personally identifiable data associated with the cardholder. This could be an account number, expiration date, name, address, social security number, etc.

Credit Card Number: (a.k.a. account number, card number or pan) Any part or all of the unique number identifying the cardholder's account which is used in financial transactions.

Credit Card Processing: The act of storing, processing or transmitting cardholder data.

PCI-DSS: Payment Card Industry – Data Security Standard defines "a set of comprehensive requirements for enhancing payment account data security…developed by the founding payment brands of the PCI Security Standards Council…to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures." (About the PCI Data Security Standard. PCI Security Standards Council, 2006. Web. 22 June 2010.)

Security Code: (a.k.a. CVV2, CVC2, card verification value or card verification code) A three-digit or four-digit number imprinted on the card that is not part of the credit card number. American Express has a four-digit number printed on the front just above the card number usually on the right side of the card. Visa, MasterCard and Discover have a three-digit code printed on the signature line on the back of the card.

Sensitive Cardholder Data: This is defined as the credit card number, expiration date, security code and data stored on track 1 and track 2 of the magnetic stripe of the card.

General Processing	**DO's**	**PCI**	**DON'Ts**	**PCI**
Section A	**A1**	**Ref.**	**A2**	**Ref.**
Applies to All Card Situations	1. Only VU employees trained in PCI compliance issues may process credit cards.	12	1. Never use a credit card process that has not been approved by the Business Office and/or IIT.	12
	2. Process all credit cards within 24 hours (or as soon as possible) or immediate if a swipe machine is available at the point-of-sale.	3	2. Never store the security code.	3
	3. Swipe the card whenever possible.	3	3. Never leave cardholder data lying out in the open.	9
	4. Process all credit cards only using an approved card swipe terminal, virtual terminal or PCI compliant software.	VU	4. The customer receipt should <u>never</u> contain: A. The full credit card number. B. The expiration date of the card. (Only the card type and the last four digits may show.)	3 & Facta 2003
	5. Provide a receipt when possible. The customer receipt should do the following at a minimum: A. Identify the place of business. B. Identify the sale with a unique number. C. Identify the date of the purchase. D. Identify the total value of the purchase. E. Identify the type of payment made.	3	5. Never accept credit cards via email, instant message or chat. These methods are not secure forms of communication.	4
	6. All receipts should only contain truncated credit card data. Whenever possible, reports or other documentation should only contain truncated credit card data.	VU	6. Minimize the acceptance of credit cards via fax.	12
	7. All terminals or merchant accounts must be settled (i.e. closed out or batched out) on a daily basis.	12	7. Cardholder data may not be moved from the department area or moved off campus without prior authorization from the Business Office. Credit Cards must be physically processed in the Business Office, Institutional Advancement or Fine Arts Center, ticketing locations. See Reports & Information Storage (Section I).	9
	8. Report any suspected theft or security breach immediately to the Business Office. Report any handling issues, no matter how small, to your supervisor.	12		
	9. All persons (excluding student workers) who process credit cards and may have access to more than one entire credit card number at any given time – staff and faculty - should pass a criminal background check processed through Human Resources.	12		
	10. Once per semester, review all policies and procedures with all individuals who handle cardholder data in any way.	12		
	11. Once per year, review all procedures and processes for vulnerabilities and implement improvements to cardholder data handling procedures.	VU		

Viterbo University
Credit Card Processing & Data Security Procedures and Policy

Approved **Methods of Card Processing**	**DO's**		**DON'Ts**	
Section B	**B1**		**B2**	
In Person	1. Process all credit cards within 24 hours (or as soon as possible) or immediate if a swipe machine is present at the point-of-sale. 2. Swipe the card if a swipe machine is available. If the magnetic strip is unreadable, you must manually enter credit card data into an approved terminal, virtual terminal or PCI compliant software. If a swipe machine in not available, enter the card information within 24 hours using Virtual Merchant. 3. Customer Receipt: A copy may be provided. 4. Destroy in-person forms that contain complete credit card data within 180 days using a cross-cut or micro shredder.		1. Never process a credit card where the name on the card does not match the individual presenting it.	
Section C	**C1**		**C2**	
Over the Phone	1. Process all credit cards within 24 hours or as soon as possible. 2. You must manually enter credit card data into an approved terminal, virtual terminal or PCI compliant software. 3. To ensure the highest level of security, the following additional items must be manually entered and submitted for approval: A. First and Last name as it appears on the card. B. The billing address. C. The zip code. D. CVV # (redacted or destroyed after being processed) 4. Use the phone order form. 5. Customer Receipt: Issued only in the FAC. 6. Destroy over-the-phone forms that contain complete credit card data within 180 days using a cross-cut or micro shredder.		1. Never process a credit card where the name on the card does not match the individual presenting it.	

Viterbo University
Credit Card Processing & Data Security Procedures and Policy

Approved Methods of Card Processing	DO's		DON'Ts	
Section D	**D1**		**D2**	
By Mail (not email)	1. Identify who opens the mail regularly and have them trained in PCI compliance issues. See Reports & Information Storage (Section I). 2. Process all forms within 24 hours or as soon as possible. Keep forms in a secure location. 3. You must manually enter credit card data into an approved terminal, virtual terminal or PCI compliant software. 4. To ensure the highest level of security, the following additional items must be manually entered and submitted for approval: A. First and Last name as it appears on the card. B. The billing address. C. The zip code. D. CVV # (redacted or destroyed after being processed) 5. Documentation: Write "Mail Order" on the form. Keep form in a secured location. 6. Customer Receipt: Issued only in the FAC. 7. Destroy mail-in forms that contain complete credit card data within 180 days using a cross-cut or micro shredder.		1. Mail-in forms created for the purpose of collecting credit card information should have the security code redacted or destroyed once they are processed.	
Section E	**E1**		**E2**	
By Web	1. Reconcile and settle batches daily or as soon as possible. 2. Customer Receipt: None issued 3. Destroy mail-in forms that contain complete credit card data within 180 days using a cross-cut or micro shredder. 4. If offices other than Business Office, Fine Arts and Institutional Advancement desire to collect and process credit cards via a website, you must contact the Fine Arts Center where they will set up a credit card collection through a third party processessor.		1. Never create a form or webpage that collects credit cards. All such pages will be actively shutdown and removed.	

Unapproved Methods of Card Processing	DO's	PCI Ref.	DON'Ts	PCI Ref.
Section F	**F1**		**F2**	
By Fax	1. If you receive a fax unexpectedly, use the "By Mail" (Section D) handling procedures for PCI compliance. Also, please inform the customer that you will accept the payment this one time and that all future payments will not be accepted by fax. Advise the customer on the preferred method your area receives credit card payments.	9	1. Never accept credit cards via fax (accept as listed in the Do's). Security of the fax is the primary concern. If you can show that data security can be maintained by locating the fax machine in a locked and isolated room with limited access or if someone is always physically present to receive the fax as it prints, you may seek an exception from the Finance Department. 2. Never accept credit cards via fax, if faxes are received, processed, and delivered in an email format.	9
Section G	**G1**		**G2**	
By Email, Instant Message, or Chat	1. If you receive an email unexpectedly, use the "By Mail" (Section D) handling procedures for PCI compliance. Consult with Technology Support Services so the email is irrevocably deleted from the email server. Please inform the customer that you will accept the payment this one time and that all future payments will not be accepted by email. Advise the customer on the preferred method your area receives credit card payments. Lastly, advise the customer for their own benefit to never share sensitive information via email. 2. If you receive an instant message, or while chatting a customer gives you a credit card number, refuse the number. Advise on the appropriate method, and inform the customer for their own benefit to never share sensitive information via IM or chat.	9	1. Never accept credit cards via email, instant message, or chat. These forms of communication are not secure.	9

Viterbo University
Credit Card Processing & Data Security Procedures and Policy

General Data Security Issues	DO's	PCI	DON'Ts	PCI
Section H	H1	Ref.	H2	Ref.
Applies to Software, Hardware or Network	1. A firewall must be used to restrict and prohibit any direct access between the internet and any network component used to store or process cardholder data. Un-trusted networks must be blocked.	1	1. Never use vendor-supplied default passwords.	2
	2. All web-based or network-based administrative access for card processing or to access cardholder data must utilize SSH, VPN or SSL encrypted communication.	2	2. No cardholder data may be transmitted over a wireless network.	VU
	3. All transmission of cardholder data across open, public networks must be encrypted using SSL.	4	3. Never use a computer to store sensitive cardholder data or to process credit cards unless it has been approved by IIT. Never use student or personal computers for storing cardholder data or processing credit cards.	VU 2, 3, 4, 5, 6, 7, 9
	4. Anti-virus and Anti-malware must be installed, up-to-date, and actively in use on computers and servers within the network. Logs must be checked regularly.	5	4. Any computer, server or hardware device that may have stored cardholder data or processed credit cards may not be re-purposed, sold, recycled, or trashed until IT has erased and reformatted all memory so that all information once stored on the machine in question is considered irretrievable.	9
	5. All critical public-facing devices, systems and databases must have the latest vendor-supplied security patches installed within one month of release.	6		
	6. All non-critical internal devices and systems must have the latest vendor-supplied security patches installed within three months of release.	6		
	7. Limit access to system components and cardholder data to only those individuals whose jobs require such access.	7		
	8. Accounts used by vendors for remote maintenance should only be enabled when needed and then disabled when no longer needed.	8		
	9. IIT must scan, test, and monitor the network for vulnerabilities once a quarter or after any significant change to the network.	1, 11		
Section I	I1		I2	
Applies to Reports & Information Storage	1. All reports generated for reconciliation purposes should contain truncated credit card data whenever possible. Only the last four digits and card type are needed.	3	1. Whenever possible, never save or store the full credit card number or expiration date. This ensures the highest level of PCI compliance.	VU
	2. All reports or documents that contain full credit card numbers must be kept in a secured area. When out of the secured area, the data must be in a folder marked "confidential," in the physical possession of a trained individual and actively being used.	9	2. Never save or store the security code.	3
			3. Never save or store credit card swipe data.	3
			4. Never dispose of reports, documents or receipts that contain cardholder data in the trash or recycle bin. The materials must be destroyed via a cross-cut shredder or micro shredder.	9
	3. Destroy all reports, documents or receipts that contain full credit card data within 180 days. If a copy must be maintained, then truncate card data by blacking it out with a black marker and then photocopy or scan the document. Save the copy and destroy the original via a cross-cut or micro shredder.	9		
	4. All reports, documents or receipts that contain full credit card numbers must remain permanently and securely stored until destroyed in the department that collected the information. If for some reason, this information needs to change physical locations, it must be hand delivered and carried in closed and sealed containers marked "confidential". Prior to the data being moved, the Business Office must grant permission for the move to occur.	9		
	5. Limit access to cardholder data to only those individuals whose jobs require such access.	7		

Viterbo University
Credit Card Processing & Data Security Procedures and Policy

Section J	J1		J2	
Offices that collect but do not process credit cards	1. All documents or receipts that contain full credit card numbers must be securely stored until forwarded to the Business Office. 2. Forward all credit card information to the Business Office as soon as possible. If the location is not on campus, forward all credit card information using overnight mail with tracking capabilities. If on campus, hand deliver the information to the Business Office. 3. Limit access to cardholder data to only those individuals whose jobs require such access.		1. Never save or store copies of the full credit card number or expiration date. If a copy must be maintained, then truncate card data by blacking it out with a black marker. This ensures the highest level of PCI compliance. 2. Never save or store the security code. 3. Never save or store credit card swipe data. 4. Never dispose of reports, documents or receipts that contain cardholder data in the trash or recycle bin. The materials must be destroyed via a cross-cut shredder or micro shredder. 5. Never transmit credit card information electronically	VU 3 3 9

<u>Offices that collect credit card information:</u>
Business Office
Fine Arts Box Office
Off-Campus Graduate Education
Graduate Education
Institutional Advancement
Mathy Center
Business Department
Ethics Department
Athletics Department

<u>Offices that Process credit cards:</u>
Business Office
Fine Arts Box Office
Institutional Advancement

Updated June 5, 2018