Credit Card Procedures and Best Practices

Credit card merchants at the university are required to follow strict procedures to protect customers' credit card data. University of North Florida credit card merchants are those colleges or departments that accept credit cards in payment of products or services. These credit card procedures and best practices include the following:

- Employees affected by PCI DSS requirements will volunteer for Training and Testing on an Annual Basis.
- NEVER e-mail or FAX credit card information.
- Do not send credit card data through campus mail or transported by hand from one department or college to another department or college.
- Process postal mail and phone order credit card payments in a secure area.
- Only employees who have a legitimate business "need-to-know" should have access to cardholder information.
- Sanitize credit card numbers on any document where the complete number is visible. Only the last four digits of the card number should be visible.
- Do not use wireless networks for the processing of Credit Cards without prior approval from the Treasury Department and ITS Security.
- Do not store credit card data on University computers, servers, laptops, or storage media such as CDs, or flash drives. If there is a business need to store credit card data, please notify the Treasury Department and ITS Security for approval and guidance.
- Do not store credit card paper data. Credit card account data must be shredded the same day it is obtained. Gathering of credit card data for processing at a later date is prohibited.
- Keep all software up to date, apply all OS updates and stay current with antivirus signatures.
- Limit Internet usage on computers that process credit cards.
- Lock computer terminals and paper storage areas when unattended.
- Do not process credit card payments for other departments or colleges.
- Include only transaction totals as supporting documentation for departmental deposits.

Important Reminders

- Any new system or software that processes credit cards OR is connected to credit card processing is required to be approved by ITS and the Treasury Department **prior** to be being acquired.
- Gateway software connections must be designed so that customers who come to a University of North Florida website to make payment via a credit

card input their credit card data on the vendor website and not a University website. There should be a direct link from the UNF website to the gateway such as Pay Path or Market Place and any interim pages or steps will not be allowed.

- Mail order forms must be designed so the part of the form that contains the customer's credit card information can be removed and shredded immediately after the credit card payment is processed. Any mail order form that requests credit card information and is distributed by a department or college MUST be approved by the Treasury Department before the form is used and/or distributed.

For additional information please contact:

Treasury Department: treasury@unf.edu

ITS Security: ITSecurity@unf.edu or submit an ITSR

Controller's Office: controlr@unf.edu