University at Buffalo
The State University of New York

Credit Card Handling Chart

Acceptable	Unacceptable
Do - Properly destroy all hardcopy forms containing cardholder data (cross cut shred, incinerate or pulp); placing in a secured bin provided by a disposal service is acceptable	Do not – Store cardholder data unless truncated (first six digits OR last four digits)
Do - Physically secure all hardcopy cardholder data pending processing	Do not – Leave cardholder information unattended on a desk, screen, or in any public area
Do – Only retain cardholder data received by phone or mail long enough to complete the transaction, then destroy the hardcopy	Do not – Send cardholder data outside of approved areas
Do – Have a unique user name and password for your work and only use it for work purposes, not personal	Do not – Share your user name, password or credentials
Do – Restrict access to devices to people duly approved and who need the access for their job	Do not – Install, move, replace or return devices without verification with Financial Management
Do – Verify the identity and credentials of all unknown persons prior to granting them access to modify or troubleshoot devices	Do not – Use any computer or mobile device to enter cardholder data that is not specifically configured and dedicated to processing payments
Do – Keep an up to date list of all credit card processing devices and inspections	Do not – Enter cardholder data online as the customer
Do - Report immediately to your supervisor and the Information Security Officer if you suspect tampering with a device or credit card information has been lost, stolen, exposed, or otherwise misused	Do not – Request or send any cardholder data by email, fax, chat, instant message, SMS, or any similar end-user messaging technology
	Do not – Store any contents of the magnetic stripe

If cardholder data is received via email, fax or voicemail:

- Destroy the sensitive data or message
- Contact the sender to inform them that this method is not secure
- Ask for the information over the phone or other compliant and secure media
- Inform the sender that UB will not accept information using this method in the future

If Financial Management has approved the need for cardholder data to be distributed internally, it must be physically secured; this includes using locked transmittal bags.

Contact An Expert

Contact	Email
Tricia Canty	tscanty@buffalo.edu
Financial Management	PCI_COMPLIANCE@buffalo.edu
PCI Compliance Committee	PCI@buffalo.edu

October 23, 2019