

## Responsibilities of Credit Card Handlers and Processors

As a credit card handler or processor for Loyola University Chicago, I agree to abide by the provisions outlined in this document and my signature acknowledges that I have read and understand the following (3) CMS documents: 1.) *Credit Card Policy*, 2.) *PCI Training Documentation*, and 3.) *Responsibilities of Credit Card Handlers and Processors*. If I need further clarification, I can refer to the Loyola University Cash Management Services (CMS) Credit Card Policies located at <https://www.luc.edu/finance/casmgm.shtml>

**I will NOT do the following:**

- 1) Acquire or disclose any cardholder’s credit card information without the cardholder’s consent, including but not limited to the full or partial 16-digit credit card number (PAN) or three- or four-digit validation code (CVV, usually located on the back of credit cards).
- 2) Request a cardholder’s PIN (personal identification number).
- 3) Transmit cardholder’s credit card information by e-mail, fax, instant message, chat or any other unencrypted form of transmission.
- 4) Electronically store any credit card information on a University computer, server or electronic USB flash drive or optical storage (e.g., CD, DVD).
- 5) Process credit card payments via cell phones, iPads, tablets or other similar devices.
- 6) Process credit card payments on the University’s wireless network unless CMS approves and provides a P2PE Point of Sale (POS) credit card device.
- 7) Share a username and password to a computer and/or application with credit card information.
- 8) Allow a 3<sup>rd</sup> party to process payments on-campus using University analog lines, Ethernet connections or Wi-Fi. I will not share my username and password with 3<sup>rd</sup> parties who come on-campus, nor will I knowingly allow third parties to use University’s guest wireless access to process credit card payments.
- 9) Leave any paper copies containing payment card data in an unsecure area.
- 10) Use a QR code linking to an eCommerce payment page without the approval of CMS.
- 11) Accept credit card payments over the phone without CMS departmental approval and procedures.
- 12) Process any credit card payments without the approval of CMS.

**I will DO the following:**

- 1) At time of employment, agree to complete a background check within the limits of local law.
- 2) Change a vendor-supplied or default password if I have access to a computer and/or application with credit card information.
- 3) Password-protect my computer if I have access to credit card data in the approved secure databases. This includes locking my workstation if I leave it unattended and using a password protected screen saver.
- 4) If I have been approved by CMS to process eCommerce payments on behalf of a cardholder, I will use both University’s LSA and RDS server and will not utilize wireless devices such as tablets or mobile phones.
- 5) Keep credit card information and POS equipment secured at all times.
- 6) Notify CMS if credit card information is stored on my computer.
- 7) Escort and supervise all visitors, including LUC personnel from other business units, into my area where cardholder information is maintained.
- 8) Store all physical documents containing credit card information and any POS credit card devices behind a **DUAL LAYER** of security (such as two of the following four locations: in a locked drawer/file cabinet, safe-which is bolted to the floor, locked office, device is secured with a tether lock, or behind a badge secured area).
- 9) Physically inspect all POS credit card devices used by my department at the periodic schedule determined by CMS.
- 10) Follow the policies and procedures set by Loyola’s CMS and ITS Department.
- 11) Report any credit card security incident immediately to my supervisor, CMS, and Information Security and Compliance, if I know or suspect credit card information has been exposed, stolen, or misused.

**I acknowledge that I have read and understood the above information, as well as the Loyola University of Chicago Credit Card Policy and PCI Training Documentation provided to me as part of this training.**

Signature	Date	New Trainee / Re-Trained Circle One
Print Name	Department, Campus	Staff / Student / Faculty Circle One