

Standards for Securing University Credit Cards and Accounts

University Standards: STN-U5351.02A

Authority

POL-U5351.02 Issuing and Using University Credit Cards policy

See Also

STN-U5351.02B Deactivating or Cancelling a University Credit Card
POL-U5315.25 Reporting Loss of University Funds or Property policy
PRO-U5315.25A Reporting Loss of University Funds or Property procedure

Purpose of Standards

These standards are to be followed by all University issued credit card holders, card custodian and approvers and enforced by the responsible Financial Manager. These security requirements apply to all University credit cards.

Protecting Credit Card Account # from Compromise and Unauthorized Use


The Financial Manager must:

- Limit authorization for the use of a department P-Card (only employees may be authorized)
- Designate an approved card holder for a department P-Card who is made responsible to follow the card holder requirements below

The card holder/user must:

- Keep the card in a secured location (must obtain written permission from the Financial Manager to keep P-cards in the card holder's wallet)
- Follow instructions to dispute a suspicious charge on payment.net statement
- Not write the P-Card # down in a separate place
- Not allow others to use his/her assigned card (or unauthorized individuals to use department P-Card)
- Not respond to email or phone requests asking for credit card numbers

Increase Security When Making On-line Purchases

- Only use reputable vendors and ensure the web site shows a business address and telephone contact
- Use secured sites where the URL of the purchase/check out webpage should start with <https://>
- Look for the secure site symbol  on the URL address bar
- Do not allow a vendor to "keep number on file"

When Employees Will No Longer Be Employed or P-Card Duties are Reassigned

The Financial Manager must ensure the Standards for Deactivating or Cancelling a University Credit Card (STN-U5351.02B) are promptly followed.

Lost or Stolen Cards/Reporting Suspected Fraud Activity

When a card is lost/stolen or fraudulent activity is suspected, the card holder must promptly notify the:

- Card Administrator in Purchasing,
- P-Card Approver (when applicable), and
- Financial Manager

Misuse/Abuse

All card holders are subject to random on-site audits. Failure to follow these guidelines places the University at financial risk and, therefore, will result in disciplinary action.