**Southern Illinois University**

**Guidelines for Credit Card Processing**

*All Merchants*

1. All credit card information must be stored in a secure area.
2. No credit card numbers can be stored on hard drive or spreadsheets.
3. Credit card information can be faxed (designated phone line only) but never emailed.
4. All old credit card information must be disposed of properly by cross-shredding.
5. Never give out credit card information to unauthorized personnel.
6. It is prohibited to store the full contents of any track from the magnetic strip in the database, log files, or point-of-sale products.
7. Do not display expiration date on receipts or merchant reports.
8. Do not store the card validation code, also called the CVC2/CVV2 number on back of the card.
9. All cardholder data printed on paper or received by fax must be protected against unauthorized access.
10. Periodically inspect credit card device surfaces to detect tampering.
11. Any credit card refund should only be processed for the original charge to the original card on the original terminal. You should keep supporting documents and all refunds should be signed off by two individuals (i.e. the employee and supervisor or fiscal officer).
12. Record retention of credit card information is 18 months.
13. Background Investigation will be performed on (new hire) credit card staff.
14. Questionnaire for PCI Compliance must be completed on a yearly basis by the manager/supervisor.
15. Update Departmental credit card procedures yearly or when changes occur.
16. Training for PCI Compliance must be completed by all staff dealing with credit cards on a yearly basis. This takes place either late spring or early summer.
17. Important website for PCI Information: <https://www.pcisecuritystandards.org/>
18. Please call Kevin Mayberry at 453-5228, for any information concerning credit cards.

*Web Based Merchants/Cashiering Systems*

1. List of Third Party service providers need to be sent to Jill Kirkpatrick or Andra Collier.
2. Third party vendors need to be PA-DSS compliant.
3. Do not use vendor-supplied defaults for system passwords and other security parameters.
4. All but the last four digits of the account number must be masked when displaying cardholder data.
5. Development, testing, and production systems must be updated with the latest security-related patches released by the vendors.
6. A virus scanner must be installed on all servers and on all work stations, and the virus scanner should be updated regularly. Per IT Security request.
7. Access to payment card account numbers must be restricted for users on a need-to-know basis.
8. All users are required to authenticate using, at a minimum, a unique username and

 password.

1. If employees, administrators, or third parties access the network remotely, they must have remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on.
2. When an employee leaves the University, that employee’s user accounts and

 passwords need to be revoked immediately.

 11. Questionnaire for PCI Compliance must be completed yearly and quarterly scans (if applicable).