Part I: Introduction of Policy and Purpose

In order to protect payment cardholders' data the Payment Card Industry has established Data Security

Credit card data shall only be transmitted electronically in encrypted forms using ITS approved computer systems.

- Sites storing credit card information on paper must be approved by Financial Administration and must comply with all PCI-DSS standards for data card information storage. A list of approved sites is included in this document.
- No paper documents, including, but not limited to paper receipts and hand written notes, containing credit card numbers or cardholder data shall be stored by unapproved departments. Approved departments would be Financial Records, Student Financial Services, Childcare and the Airpark. They will store the data in a safe, secure and locked pl

these documents must

Part V: Roles and Responsibilities

It is the responsibility of every employee of the University handling credit card information to be aware of the potential of fraud and theft of cardholder information and to do their part in protecting our customers from experiencing a loss due to the mishandling or misuse of their credit card information.

Each department that processes this type of data is required to designate a staff person who is responsible for the collection and proper handling of cardholder data. This individual will:

- Be required to attend University provided training on the appropriate handling of cardholder data. The employee will be required to sign a form indicating the time and date of training and the understanding of their responsibility.
- Be responsible for limiting access to this data by other employees and ensuring that employees who handle this data are trustworthy and know the proper policies and procedures for handling cardholder information.

In addition, Departments with credit card terminals are responsible for:

- Limiting access to the terminal to authorized personnel only.
- Monitoring the activity on the machine and reporting any suspicious activity immediately. See Incident Process Part VII.

The office of Financial Administration in conjunction with the office of the CIO is responsible for overseeing all aspects of information security, including but not limited to:

- Creating, maintaining and distributing security policy and procedures.
- Incident planning and response for incidents involving merchant terminals and non-electronic handling of credit card information.
- Training and awareness programs.

The CIO shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS including:

The Human Resource Office is responsible for tracking employee participation in the security awareness program including

- Facilitating participation upon hire and at least annually
- Ensuring that employees acknowledge in writing at least annually that they have read and understand the company's Payment Card Acceptance Policies and Procedures
- Screen potential employees prior to hire to minimize the risk of aad.6n)/TT11IntTD0Tcnf1.42320TD0Tc8.2190TD0.0036c(to)