Section Number: _____	Section Header:
Subject: __PCI DSS Information Security Policy	Effective Date: __DRAFT __
Responsible Office: __Information Technology _	Responsible Officer: ___Judith R. Galang_____

PCI DSS Information Security Policy DRAFT

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of requirements for enhancing payment account data security. Compliance with the standard is mandatory and the University must abide by these requirements to limit its liability and continue to process credit card payments.

Purpose

The purpose of this policy is to establish guidelines for departments to implement data protection standards to ensure compliance with the PCI DSS.

Scope

This document applies to all faculty, staff, students, and external vendors. Any department that wishes to accept, process, transmit, or store credit card data must follow this policy. All equipment, including point of sale terminals, workstations, servers, and computers also fall into the scope. This policy applies to all credit card transaction types including in-person, telephone, mail, and online payments.

Policy

ents

through the centralized merchant contract. University standard web applications are in place as the preferred method for acceptance of online credit card payments. Any department that wishes to accept credit card payments using other methods must validate their compliance with the PCI DSS prior to gaining authorization from the Office of the Controller.

5. Sensitive authentication data must be masked or shredded immediately after processing.

Online Payment and Electronic Storage

1. Departments that
   application should contact the Office of Campus Information Systems to establish an account.
2.
   application must submit proof of compliance with the PCI DSS to the Office of the Controller prior to being authorized to process credit card payments.
3. Third party payment applications must comply with the Payment Application Data Security Standard (PA-DSS).
4. If all payment transactions are outsourced to an external vendor, the NJCU

Masking - Method of concealing a segment of data when displayed. Masking is used when there is no business requirement to view the entire PAN.

Merchant For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

Contact

Any questions or concerns related to these procedures can be directed towards the Offices of Risk Management, Controller, or PeopleSoft Security Administrator.

Related Documents

Information Privacy Policy
Responsible Use of Computing Resources
General Principles and Guidelines