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

New Jersey City University's preferred method for acceptance of credit card payments 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.

General Requirements

1. Access to Cardholder Data and System Components should be limited to only those individuals whose job requires such access.
2. Any job position that requires access to stored Cardholder Data will be considered security sensitive. Background checks must be performed for any person prior to assignment of duties that includes access to stored Cardholder Data.
3. Individuals processing credit card transactions on a regular basis must attend data security protection training every year. Individuals who accept or process credit card payments on a temporary basis are recommended, but not required, to attend this training.
4. Any person processing credit card information must sign a disclosure form agreeing not to disclose or acquire any information concerning a cardholder's credit card account without the cardholder's consent.
5. Sensitive Authentication Data must never be stored in any place.
6. Credit card numbers should never be stored on a personal computer.
7. Credit card numbers should never be transmitted via unencrypted email or any other unsecured transmission method.
8. A self-assessment questionnaire must be completed annually by the University and by individual departments not following the preferred methods of payment processing.
9. Appropriate segregation of duties between credit card processing, the processing of refunds, and the reconciliation function must be established.

Procedures and Additional Transaction Type Requirements

Hard Copy Processing

1. Physical cardholder data must be secured in a locked area with access limited to personnel required to access that data.
2. Credit card numbers should be masked using methods such as blacking out all but the last four digits.
3. Credit card information should not be retained longer than what is necessary for business, legal, or regulatory purposes.
4. Documents containing credit card numbers must be shredded before being disposed.

Point of Sale (POS) Terminals

1. Cardholder data should not be stored on the terminals.
2. Printouts should not include the entire credit card number.
3. New POS terminal sales must be certified PCI compliant prior to purchase.
4. Existing POS terminals must be validated to be PCI compliant or replaced.

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

Online Payment and Electronic Storage

1. Departments that wish to utilize the University's preferred online payment application should contact the Office of Campus Information Systems to establish an account.
2. Departments that do not want to utilize the University's preferred online payment 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 department is responsible for verifying that the external vendor is PCI compliant.
5. All electronic machines involved with the processing, transmission, or storage of cardholder data are subject to network vulnerability scans on at least a quarterly basis.

Enforcement

Departments not complying with this policy may lose the privilege to accept credit card payments. Additionally, fines may be imposed by the affected credit card company or the acquiring bank. Those in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary actions, suspension, termination of employment and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

Definitions

Cardholder Data – At a minimum, cardholder data contains the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following:

- Cardholder name
- Expiration date
- Service Code

Sensitive Authentication Data – Security-related information (card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.

System Components – Any network component, server, or application included in or connected to the cardholder data environment.

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