JACKSONVILLE STATE UNIVERSITY

Manual of Policies and Procedures

POLICY NO.: VII:03 **DATE: April 2021**

REVIEW/REVISION DATES: TBD

SUBJECT: Processing Card Industry (PCI) Compliance

APPROVED: Dr. Don C. Killingsworth, Jr., President

PURPOSE

This document prescribes the policy, responsibilities, and procedures to ensure the proper handling of cardholder data for all JSU units that accept credit card information.

This policy serves as an addendum to all other information technology policies to provide additional protections to card holder data.

OVERVIEW

JSU handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations, and to guard the future of the organization.

JSU commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end the University is committed to maintaining a secure environment in which to process cardholder information to meet these promises.

POLICY

1. Protect Stored Card Data

All sensitive cardholder data stored and handled by JSU and its employees must always be securely protected against unauthorized use.

- Sensitive card data that is no longer required by JSU for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Primary Account Number), it must be masked when displayed.
- PAN'S which are not protected as stated above must not be sent to the outside network via unsecure end user technologies e.g., instant messaging, chats, unencrypted email etc.

- **It is strictly prohibited to store:**
    - The contents of the payment card magnetic stripe (track data) on any media whatsoever.
    - The CVV/CVC (the 3- or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
    - The PIN or the encrypted PIN Block under any circumstance.

2. Access to the sensitive cardholder data

All access to sensitive cardholder data must be controlled and authorized. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder data must be restricted at a minimum of the first 6 or the last 4 digits of the cardholder data.
- Access rights to privileged user ID's must be restricted to employees necessary to perform job responsibilities.
- Privileges must be assigned to individuals based on job classification and function (Role based access control).
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees who have a legitimate need to view such information.
- No other employees will have access to this confidential data unless they have a genuine business need.
- JSU will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- JSU will ensure there is an established process including proper due diligence is in place before engaging with a Service provider.
- JSU will have a process in place to monitor the PCI DSS compliance status of the Service provider.

3. Physical Security

All POS and PIN entry devices must be appropriately protected and secured so they cannot be tampered or altered.

- A list of devices that accept payment card data must be maintained.
    - The list must include make, model, and location of the device.
    - The list must have the serial number or a unique identifier of the device.
    - The list must be updated when devices are added, removed, or relocated.
- POS devices must be periodically inspected to detect tampering or substitution.
- Personnel using the devices must be trained and aware of handling the POS devices.

- Strict control is maintained over the external or internal distribution of any media containing card holder data and must be approved by the Office of Information Security.
- All computers and related devices that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorized use.

4. Protect Card Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc.) must never be sent over the internet via email, instant chat, or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it must be done after authorization from the Office of Information Security and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorized by the Office of Information Security, logged, and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

5. Disposal of Stored Card Data

All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.

- JSU will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials be crosscut shredded, incinerated, or pulped so they cannot be reconstructed.
- JSU will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted (e.g., through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media);
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” and access to these containers must be monitored.

6. Security Awareness

- All personnel who handle processing card information must complete annual security training on protecting card data.

7. Processing Card Network Security

All systems that process card holder data must reside in a controlled network security zone.

- Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment.
- Stateful Firewall technology must be implemented where the Internet enters JSU Card network to mitigate known and on-going threats.
- All inbound and outbound traffic must be restricted to that which is required for the card holder data environment.
- All outbound traffic must be authorized by the Office of Information Security (i.e., what are the whitelisted category of sites that can be visited by the card holder environment)
- No direct connections from Internet to cardholder data environment will be permitted. All traffic must traverse through a firewall.

8. Secure Device Compliance

All information systems that process, transmit, or store card holder data must be configured in accordance with the applicable standard for that class of device or system. Standards must be written and maintained by the team responsible for the management of the system, in conjunction with the Information Security Office. System configurations should be updated as new issues are identified.

- All vendor default accounts and passwords for the systems must be changed at the time of provisioning.
- All users with access to card holder data must have a unique ID.
- All the logs generated from the antivirus solutions must be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- Quarterly internal vulnerability scans must be performed by JSU internal staff or a 3rd party vendor, and the scan process must include that rescans will be done until passing results are obtained, or all “High” vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by JSU’s internal staff.
- The scan process should include re-scans until passing results are obtained.

9. Third party access to card holder data

All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).

- All third-party companies providing critical services to JSU must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with JSU's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:
    - Adhere to the PCI DSS security requirements.
    - Acknowledge their responsibility for securing the Card Holder data.
    - Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
    - Have appropriate provisions for business continuity in the event of a major disruption, disaster, or failure.
    - Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.
    - Provide a report to the Chief Information Officer annually:
        - SOC report from an independent certified public accountant
        - PCI certification from an independent party

11. Roles and Responsibilities

- Information Security Officer is responsible for overseeing all aspects of processing card security, including but not limited to:
    - Creating and distributing card holder data security policies and procedures.
    - Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel.
    - Creating and distributing processing card security incident response and escalation procedures

- The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

- System and Application Administrators shall
    - Maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation.
    - Monitor and analyze security alerts and information and distribute to appropriate personnel.
    - Administer user accounts and manage authentication.

    - Monitor and control all access to data.
    - Maintain a list of service providers.
    - Ensure there is a process for engaging service providers including proper due diligence prior to engagement.

- The Human Resources 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 JSU's information security policy.

- The JSU Business Office (or equivalent) shall maintain operational procedures that are consistent with and enforce the PCI policies and data protection requirements set forth.

- University Counsel will ensure that for service providers with whom cardholder information is shared:
    - Written contracts will require adherence to PCI-DSS by the service provider.
    - Written contracts will include acknowledgment or responsibility for the security of cardholder data by the service provider.

RESPONSIBILITY

The Chief Information Officer is responsible for this policy.

EVALUATION

This policy will be reviewed at least every five (5) years by the Chief Information Officer.