JACKSONVILLE STATE UNIVERSITY

Manual of Policies and Procedures

POLICY NO.: VII:01 **DATE: June 2021**

REVIEW/REVISION DATES: TBD

SUBJECT: Information Technology Security Policy

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

PURPOSE

This policy encompasses all aspects of information security to the Jacksonville State University (JSU) network and information systems.

Effective security is a team effort involving the participation and support of every JSU employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

POLICY

Security Awareness and Procedures

The policies and procedures outlined within this policy must be incorporated into JSU practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into daily JSU practice.
- Distribute this security policy document to all JSU employees to read. It is required that all employees confirm that they understand the content of this security policy document.
- All employees who handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with JSU.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- JSU security policies must be reviewed and updated as needed.

Acceptable Use Policy

The purpose of publishing an Acceptable Use Policy is designed to ensure the University is committed to protecting the employees, partners, and JSU from illegal or damaging actions by individuals, either knowingly or unknowingly. See posted Acceptable Use Policy here.

All JSU employees are required to acknowledge and sign the Acceptable Use Policy (AUP).

Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- Employees must have appropriate credentials and be authenticated for the use of technologies.
- Employees must take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees must ensure that technologies are used and set up in acceptable network locations.
- Personnel using the devices must verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices must be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel.
- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on JSU sites.
- Media is defined as any printed or handwritten paper, received faxes, back-up tapes, computer hard drive, jump drive, etc.
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where sensitive data is accessible.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorized.
- Strict control is maintained over the storage and accessibility of media.

Network security

- Firewalls must be implemented at each internet connection and any demilitarized zone and the internal JSU network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols, and ports, including a business justification.
- 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. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments, such as the business network, and open network.
- All inbound and outbound traffic must be restricted to that which is required for the data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions must be documented.

- 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).
- JSU will quarantine wireless users into a DMZ, where they will be authenticated and firewalled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment must be documented and must be updated in accordance with the changes in the network.
- The firewall rules will be reviewed on a six-month basis to ensure validity, and the firewall must have clean up rule at the bottom of the rule base.
- All external traffic must traverse through a firewall.

Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

- Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to JSU if disclosed or modified. Confidential data includes cardholder data.
- Internal Use data might include information that the data owner feels should be protected to prevent unauthorized disclosure.
- Public data is information that may be freely disseminated.

Disposal of Stored Data

All data must be securely disposed of when no longer required by Public Universities of Alabama Records Disposition Authority (found here) regardless of the media or application type on which it is stored.

- An automatic process must exist to permanently delete on-line data, when no longer required.
- 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.

Processing Card Industry Compliance

For additional policies and guidelines related to Processing Card Industry (PCI) refer to Policy VII:03 Processing Card Industry (PCI) Compliance here.

Roles and Responsibilities

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

    - Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).

- The Information Technology Division shall maintain daily administrative and technical operational security procedures (for example, user account maintenance procedures, and log review procedures).

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

Disciplinary Action

Violation of the standards, policies, and procedures presented in this policy by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions, or using poor judgment will not be used as excuses for noncompliance.

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.