JACKSON STATE UNIVERSITY'S
Phishing /SPAM Solution and Management Program
(In compliance with Cybersecurity Maturity Model Certification 2.0 (CMMC)

I. Phishing /SPAM Solution and Program Purpose

This document summarizes the Jackson State University's (the "University's") comprehensive written Phishing and SPAM solution and Management program (the "Program"). In particular, this document describes the Program process used by JSU IT staff and members of the CSIRT team to create a safe, educational environment for JSU employees and students to practice phishing email identification with no penalty to them if a link is clicked.

II. Definitions

Phishing- means all information required to be protected under the Gramm-Leach-Bliley Act ("GLB Act"). "Covered data" also refers to financial information that the University,

SPAM- means all information required to be protected under the Gramm-Leach-Bliley Act ("GLB Act"). "Covered data" also refers to financial information that the University,

Vishing- means all information required to be protected under the Gramm-Leach-Bliley Act ("GLB Act"). "Covered data" also refers to financial information that the University,

III. Phishing /SPAM Solution and Program Objectives

The GLBA, FERPA Acts and CMMC requires the University develop, implement and maintain a **Phishing /SPAM Solution and Program** containing a solution for phishing an SPAM that helps JSU employees and students become prepared to recognize and report phishing attempts through awareness trainings, phishing campaigns and simulations. This program and solution will implement technical control solutions, and employee training and awareness for phishing protection with the following objectives:

- Train JSU employees and students to recognize, report, and avoid phishing attacks, which helps protect them from cyber-threats.
- Help the JSU Division of Information Technology IT and its CSIRT team members collect better metrics and information about email-based attacks in order to better protect the JSU community from these threats.
- Identify and apply essential technical controls to prevent phishing attacks and SPAM
- Mitigation of and response to reported phishing attacks
- Maintaining and adjusting this Phishing Program based upon the results of testing and monitoring.

IV. Phishing /SPAM Solution and Program Coordinator(s)

A. Designated Representatives: The University's Chief Information Security Officer and/or Information Security Officer are designated as the Program Officer(s) who shall be responsible for coordinating and overseeing the JSU Phishing/SPAM solution and management Program along with the University's Chief Information Officer and Chief Technology Officer. Duties of the Program Officer(s) include:

1. Coordinate with responsible parties to ensure adequate training and education is developed and delivered for all employees and students
2. Collaborate with the University's Division of Information Technology to assess procedures for monitoring phishing/SPAM reports and attacks
3. Review existing policies, standards and guidelines that provide for phishing/SPAM protection and make recommendations for revisions as appropriate

B. Scope of Program: The Program applies to any phishing attacks or attempts via a JSU assigned email to employees, students, vendors or contractors and can be extended to include Smishing and Vishing or any other forms of phishing as needed as identified by University phishing metrics and phishing data trends.

V. Gathering Baseline Click Rate Metrics

A. Phishing Baseline Assessment: The University will launch a Phishing Simulation Campaign to collect baseline metrics of existing employee-related risk data regarding: 1) Phishing rates, 2) Rates of recognizing fraudulent attempts to obtain sensitive student or employee data, 3) Rates of reporting suspicious emails and activity. The phishing simulation can be conducted internally (using tools such as GoPhish) or externally (ex. Terranova Security Phishing tournament) This baseline data will be used to:

1. Focus training materials on specific high risk areas for employees and students
2. Serve as a metric for initial click rate
3. Benchmark for evaluating the effectiveness of phishing awareness training course

VI. Raising Employee and Student Awareness

Phishing /SPAM Solution and Program coordinator(s) will implement the following phishing based strategies and activities to help raise awareness among JSU employees and students:

A. Employee and Student Phishing/SPAM Training

Existing, and New, Employees and Students will be provided the following Phishing Training:

- **Cyber Awareness Training-** will include the following phishing information:

    1. What is phishing and how it happens
    2. Top 10 Tips to Avoid Phishing/SPAM
    3. Anatomy of a phishing email
    4. Actions to take before or After clicking a suspicious link
    5. The when, what, how and who of reporting phishing emails or attacks (email report phishing and spam options available)
    6. Information about phishing risks and data breaches

- **Verification and Tracking of Training Compliance-** To track training information each employee will sign into CANVAS to complete Cyber Awareness and Phishing Training along with submitting electronic acknowledgement statements that verify that the employee has:

    1. Reviewed the training materials
    2. That he/she understands the content presented in the trainings
    3. That he/she acknowledges that they have taken the training and are aware of their responsibilities. Acknowledgement statements must be submitted in the training modules before the training are considered complete.

B. Employee and Student Phishing/SPAM Campaign

Existing, and New, Employees and Students will be provided the following Phishing Campaign materials via email or will be accessible from the JSU IT Cyber security website page to help bring awareness to phishing attempts and attacks:

1. Phishing Flyers
2. Downloadable phishing tip sheets
3. Phishing focused videos

VII. Application of Phishing /SPAM and Spoofing Solution Controls

In addition to the Phishing/SPAM program a Phishing /SPAM Solution(s) will be applied to JSU student and employee emails to add to our defenses against Phishing and spam. The tool will filter, scan, and block external malicious emails as follows:

1. Google work space spam filters designed to identify incoming dangerous emails and give no-click/download alerts, and scan email attachments
2. Phishing Report/Friendly Reminder emails detailing real phishing emails received by University employees
3. DKIM signatures
4. Sender Policy Framework (SPF)
5. Domain-based Message Authentication, Reporting, and Conformance (DMARC) records

VIII. Program Monitoring and Reporting

A. Monitoring

Monitoring of the University's Phishing /SPAM program will be conducted by the program coordinator(s) and email administrator. The level of monitoring will be appropriate based upon the frequency of end user reported phishing cases.:

1. Google work space spam filters designed to identify incoming dangerous emails and give alerts, and scan email attachments
2. Phishing Report/Friendly Reminder emails detailing real phishing emails received by University employees
3. DKIM signature,
4. Sender Policy Framework (SPF)
5. Domain-based Message Authentication, Reporting, and Conformance (DMARC) records

B. Reporting

The Program Coordinator(s) will provide a report on the effectiveness of the Phishing/SPAM program information via Phishing Simulation Reports

IX. Program Maintenance

The Program Officer(s)is responsible for evaluating and adjusting the Program solutions and materials based on assessment activities undertaken pursuant to the Program.