JACKSON STATE UNIVERSITY'S
Vendor Management Plan/Program

I. Vendor Management Plan Purpose

This document summarizes the Jackson State University's comprehensive vendor management program (the "Program"). The vendor management program is divided into two phases and will be guided by the vendor management framework.

II. Definitions

"**Vendors**" refers to all third party entities who are considered high critical risk providers that provide products and services essential to JSU's core business functions.

III. Vendor Management Program Overview

The vendor management program is divided into two parts 1) initial set up of the program and 2) ongoing monitoring of vendors

PHASE I

IV. Initial Stage-The first phase of the JSU Vendor Management program will include the gathering of information on the identified list of vendor(s) of interest, collection of documentation and service agreements and identify risks created by JSU's use of identified high critical risk vendors as it relates to laws and regulations that Jackson State University must adhere to in order to ensure that its' critical data sets are protected from data breaches, misuse, and other malicious attacks**.**

Vendor Management Program Components- JSU's Vendor Management Program will have five components: (1) Identifying the risks created by JSU's use of identified high critical risk vendors (2) Defining policies and procedures for monitoring vendors (3) Create and consolidate JSU's existing vendor profile data and documentation into a single repository (4) maintaining and adjust Vendor relationship data upon renewal or termination of vendor contract with Jackson State University.

V. Identifying and defining JSU's risks: Jackson state University faces the following risks as a result of its' third party relationships:

- Operational risk – This can include a significant system outage of the service that may not be back online within 24 hours.
- Financial risk – The actions of the vendor may place the organization at financial risk. Suppose the Service Level Agreement is not upheld. This risk might manifest as lost revenue or paying for rework, litigation or regulatory fines.
- Reputational risk –Vendor's inability to prevent breaches and uphold its' SLA may cause damage to JSU's reputation.
- Regulatory risk – This risk relates to specific laws and rules that may be broken if there is misleading information provided to JSU students and employees by a third party vendor. JSU risks being responsible for a direct regulatory violation.

VI. Defining policies and procedures for monitoring vendors: Vendor Performance will be monitored by policies and procedures outlined in the Jackson State Third Party Vendor Management Security Policy 50000.023. Additional monitoring may include but are not limited to the following standards:

- Performance - Service Levels, Uptime Statistics
- Vulnerabilities – Monitor vulnerabilities for vendor's specific products and services by checking vulnerability databases

VII. Centralized list of high risk vendors: A centralized list of vendors that provide core business services and functions to Jackson State University will be compiled along with the following company profile information:

- Vendor Name
- Vendor Purpose (services they provide)
- Vendor Contact Info (phone, email, and address)
- Who Manages the Vendor Relationship?

VIII. Due Diligence

The University intends, as part of the Vendor Management Program, to check for the appropriate documentation and reports to validate and ensure that the external and internal risks and impacts to the security, confidentiality, and integrity of JSU's core business services and its' critical data sets are minimal.

- Current Vendors will provide reports and documentation such as financial reports and SOC reports etc. to provide evidence as validation as it relates to the services they provide to the university.

- A new Vendor's good standing and licensing to conduct business will be determined. The vendor will also be required to provide reports and documentation such as financial reports and SOC reports etc. to provide evidence as validation as it relates to the services they provide to Jackson State University.

PHASE II

IX. Ongoing Monitoring

Monitoring will be conducted to reasonably ensure that vendors are capable of maintaining the appropriate safeguards for JSU's critical data sets, and to swiftly detect and correct breakdowns in security. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring may include notifying /coordinating with vendor on essential system updates and patches, checking for vulnerability alerts on vendor product(s), system up/downtime and other reasonable measures adequate to verify that proper security controls, systems and procedures are working.

X. Roles and Responsibilities

The Chief Information Officer, Chief Technology Officer and Chief Information Security Officer shall coordinate with those responsible for the third party service procurement activities, and the management of the third party vendor relationship as it pertains to IT provided services, and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those vendors that are capable of maintaining appropriate safeguards for JSU's critical data sets.

XI. Program Maintenance

The CISO,CIO, and CTO are responsible for evaluating and adjusting the Program based on the risk identification and review of assessment activities (collection of documents and reports) undertaken pursuant to the Program, as well as any material changes to the University's operations or other circumstances that may have a material impact on the Program.

XII. Policies, Standards and Guidelines

The University has adopted comprehensive policies, standards, and guidelines relating to information security. They are incorporated by reference into this Vendor Management Plan, and include:

Policies: Third Party Vendor Security Policy 50000.023

VERSION	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR/Editor
V1.0	09/03/2021	New Document	S. Nichols
V1.1	05/25/2022	Update made to grammar and added more responsible IT employees	S. Nichols
V1.2	03/16/2023	Updated verbiage to initial stage and added the creation of a vendor list as initial step	S. Nichols