Policy Name	Third Party Vendor Security Policy
Policy Number	50000.023
Effective Date	May 25, 2020
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	March 11, 2022

1. Policy Statement

The purpose of this policy is to establish rules and operating parameters for third party vendors' access to University critical information, their operator responsibilities, and protection of Jackson State University's assets, data, and PII. This policy supports compliance with federal and state data privacy laws.

2. Definitions

2.1. PII- **Personally Identifiable Information** can include information such as phone numbers, social security numbers, credit or bank account numbers, and addresses.

2.2. Passphrase- A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*

3. Employee Adherence

This policy applies to all JSU employees, contractors, consultants, internal and external vendors, including all personnel affiliated with third parties who access and use JSU services through resources it provides such as the JSU Website(s), and Mobile Apps, etc.

4. Policy

4.1. **General Policy**

Prior to entering into any agreement or contract, Jackson State University employees shall follow due diligence in selecting third party vendors. Third parties must comply with all applicable state procurement, JSU policies, practice standards, and agreements as well as any binding legislation at the state and federal levels. This policy supports law in certain areas but shall not replace any potential changes in current or future compliance components levied against third party vendors through statute, law, or contract.

4.2. **General Vendor Responsibilities**

Third party vendors shall provide JSU a point of contact for contract terms and service offering implementation. A JSU point of contact will work with the third party vendors to ensure the vendor is in compliance with all state and federal laws as well as this policy.

4.3. **Third Party Security Controls**

4.3.1. JSU employees, vendors and contractors should not use the same password(s) for JSU accounts as passwords for access to other non-JSU accounts (e.g., personal ISP account, benefits, etc.).

4.3.2. Data and personnel confidentiality terms shall protect all JSU Confidential Information and PII.

4.3.3. Service providers shall provide JSU with a list of all staff working on the contracted services. The list shall be updated and provided to JSU within twenty-four (24) hours of staff changes.

4.3.4. Ensure industry acceptable application development security standards (e.g. OWASP) are followed so that IT systems and applications are tested and secured in every step of the application and system development life cycle.

4.3.5. Ensure firmware, software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.
4.3.6. Password fields should display only masked characters as the user types in their password, where technically feasible.
4.3.7. Service provider access shall be uniquely identifiable and password/access management must comply with all JSU requirements
4.3.8. Vendor data privacy and information security procedures and protocols shall be made available and meet JSU's requirements for the return, destruction, or disposal of information in the service provider's possession at the end of the agreement.
4.3.9. The service provider shall only use JSU's information and systems for the purpose of the direct business agreement. No other uses are allowed unless expressly granted in writing by JSU.

4.4. **Third Party Operation Management**

4.4.1. Providers who provide infrastructure and platform hosting services should ensure non-JSU authorized personnel cannot physically or electronically inspect, insert, share, access, steal or change content JSU's assets, including without limitation JSU's used network, traffic, infrastructure, applications, RAM and storage space.
4.4.2. Data destruction processes should follow a process that securely wipes all data on all media using a method that will not allow data to be retrieved. For all IT systems that access Regulated, Confidential, or Personal Information, JSU requires the destruction be performed in accordance with NIST Special report 800-88.

4.5. **Third Party Compliance (Credit Card Data)**
4.5.1. Vendors should secure all Credit Card data in accordance to requirements listed in the most current and release editions of the Payment Card Industry – Data Security Standards (PCI-DSS or PCI).
4.5.2. Vendors should use additional security protection controls for protecting against access to JSU's Regulated, Personal, or Confidential information, such as:
• Web application firewalls, intrusion detection and protection systems, data loss prevention systems, strong passphrases, etc.

5. Policy Compliance
5.1. Any JSU employee, vendor(s) and contractor(s) found to have violated this policy may be subject to disciplinary action, up to and including revocation of access privileges, or termination of contract or employment. In addition to University discipline, users may be subject to criminal prosecution under federal, state or local laws; civil liability or both for unlawful use of any IT System.

6. Related Standards, Policies, and Processes
- Password Policy 50000.021

7. Revision History
- Policy Created: May 25, 2020
- Revised: August 10, 2021
- Revised: March 11, 2022
-