Policy Name	Data Security Policy
Policy Number	50000.008
Effective Date	March 29, 2019
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	April 20, 2020

1.0 Policy Statement

Jackson State University's ("JSU" or "University") Department of Information Technology ("DIT") intention for publishing a Data Security Policy is to identify, define, and outline data and how to securely handle, discard, and report the inappropriate use of University data. Certain types of data are protected by law and have a high security risk if improperly handled. This policy outlines the University's requirements for handling and disposing of this data.

2.0 Purpose

The purpose of this policy is to define the various types of data and identify acceptable security measures that should be applied when handling Restricted data such as, Personal Identifiable Information, Student and Employee Financial data and Personal Health Information as required by the HIPAA, FERPA, GLBA Acts, as well as public University Data in electronic and paper formats.

3.0 Definitions

3.1 University Data - University data (electronic and paper) consists of information stored in any college database or on paper that contains information on past, current, or future students, employees, donors or friends. All University data, whether maintained in a central database or copied into other data systems, remain the property of the University and are governed by this policy statement.

3.2 Data Ownership - JSU is considered the data owner of all institutional data; individual units or departments may have stewardship responsibilities for portions of the data.

3.3 Data Users - Individuals who need and use University data as part of their assigned duties or in fulfillment of their role in the University community.

3.4 Confidential data - data which is legally regulated; and data that would provide access to confidential or restricted information.

3.5 Restricted data - data which DIT has not decided to publish or make public; and data protected by contractual obligations.

3.6 Public data - data which there is no expectation for privacy or confidentiality.

3.7 Student Employees - an independent contractor and is not eligible for University fringe benefits including retirement, medical insurance, FICA matching contribution, etc.

4.0 Employee Adherence

This policy applies to University Faculty, Staff, and Student Employees.

5.0 Policy

5.1 In compliance with the safeguard rules of the FERPA and GLBA acts no member of the JSU community is permitted to electronically store or maintain credit card or debit card numbers, expiration dates, and/or security codes in any way relating to JSU or JSU-sponsored activities.

DIT or must approve the use of any system or application that electronically processes, stores, or transmits credit card data.

5.2 Paper documents containing credit card data should be secured in a locked office and stored in a cabinet. In an open office environment paper documents should be stored in locked cabinets. Paper documents should not be left in an unsecured office after work hours.

5.3 All credit card processing (e.g., online, phone, mail, over-the-counter, card-swiping) must be reviewed and approved by the Executive Director of the Business Office.

5.4 The following confidential data types can only be electronically stored on a DIT managed server and can only be accessed from a DIT managed computer.

- Social Security number
- Driver's License number
- State/Federal ID Card number
- Passport number
- Financial account numbers (checking, savings, brokerage, CD, etc.)

5.5 In the event that an exception is necessary in order to carry out the business of the University, the user must get written approval from both his/her Vice President as well as the Information Security Officer.

5.6 It is recommended that all other confidential data and restricted data types be electronically stored or accessed from the one of the following list of devices, in order of preference:

- DIT managed server
- DIT managed desktop computer
- Encrypted laptop
- Encrypted mobile storage device

5.7 Any encrypted device must be encrypted using a process documented and approved by DIT and the administrator of such system must report to the Information Security Officer on system security related matters.

5.8 When handling physical documents containing any Confidential and/or Restricted data types, the documents must be in your possession at all times; otherwise they should be stored in a secure location (e.g. room, file cabinet) to which only specifically-approved individuals have access through lock and key.

5.9 When the information is no longer needed, the physical documents must be shredded using a University-approved device prior to being discarded; or destroyed by a University-approved facility.

5.10 Confidential data and restricted data should not be taken or stored off-campus unless the user is specifically authorized to do so by a Vice President and notification of the authorization is sent to the Information Security Officer.

5.11 JSU reserves the right to electronically scan all University-owned resources and resources connected to the Jackson State network for confidential data. In event that confidential data is found in unauthorized locations, the Information Security Officer will follow-up with the responsible Vice President to remedy the situation.

5.12 Confidential data cannot be transmitted through any electronic messaging (i.e. email, instant messaging, text messaging) even to other authorized users.

5.13 Confidential data in a physical format cannot be transmitted through untracked delivery methods. Campus mail and regular postal services are not tracked delivery methods.

5.14 All faculty, staff, and student University account passwords must be complex. A complex password is defined as follows:

5.14.1 Passwords must be at least ten or more characters long.
5.14.2 At least one capital letter.
5.14.3 At least one special character.

University passwords will expire after 90 days.

Users who are authorized to access or maintain confidential data or restricted data must ensure that it is protected in accordance to the safeguard rules of the GLBA, FERPA, and HIPPA Acts to the extent required by Jackson State policy or law after they obtain it. All data users are expected to:

Under the GLBA and FERPA Acts:

5.14.4 Access restricted PII data only to conduct University business.
5.14.5 Request only the minimum confidential data or restricted data necessary to perform their University business.
5.14.6 Respect the confidentiality and privacy of individuals whose education and financial records they may access.
5.14.7 Observe any ethical restrictions that apply to data to which they have access.
5.14.8 Know and abide by applicable GLBA and FERPA laws or policies with respect to access, use, or disclosure of data.
5.14.9 Immediately notify the appropriate security officials, and individuals in the event a data breach occurs.

Under the HIPAA Act:

5.14.10 Access restricted PII data only in their conduct of University business.
5.14.11 Request only the minimum confidential data or restricted data necessary to perform their University business.
5.14.12 Respect the confidentiality and privacy of individuals whose education and financial records they may access.
5.14.13 Observe any ethical restrictions that apply to data to which they have access.
5.14.14 Know and abide by applicable HIPPA laws or policies with respect to access, use, or disclosure of data.
5.14.15 Keep safeguards in place to ensure that student PHI and medical records remain confidential.
5.14.16 Only disclose or release a student’s medical records to University officials as necessary or in event of an emergency.

5.14.17 Immediately notify the appropriate security officials, and individuals in the event a data breach including a student's PHI or restricted data occurs.

6.0 Policy Compliance

6.1 Compliance with these data protection policies is the responsibility of all members of the University community.

6.2 Violations of these policies will be dealt with seriously and will include sanctions, up to and including termination of employment.

6.3 Users suspected of violating these policies may be temporarily denied access to the data as well as University information technology resources during investigation of an alleged abuse.

6.4 Violations may also be subject to prosecution by state and federal authorities.

6.5 Suspected violations of JSU's data protection policies must be reported to the Information Security Officer.

7.0 Related Standards, Policies, and Processes

- ➢ Data Security Definitions
- ➢ Data Security Classifications

8.0 Revision History

- ➢ Policy Created: December 7, 2015
- ➢ Revised: February 2, 2016
- ➢ Revised: February 13, 2019
- ➢ Revised: April 20, 2020