Policy Name	Data Security Definitions
Policy Number	50000.002
Effective Date	December 7,2015
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	February 13, 2019

1.0 Policy Statement

Jackson State University (JSU) has outlined key terms and terminology to assure that all of its employees, units, and departments clearly understand what their role and responsibilities are when handling university data as data custodians, and managers.

2.0 Purpose

This policy is intended to define terminologies used to create JSU's data security standards and guidelines to protect student records and data.

3.0 Definitions

Computing Equipment	Any electronic storage device, laptop, or system.
Data Custodian	Individuals responsible for providing a secure infrastructure in support of University Data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized and implementing and administering controls over the information. In many cases at Jackson State, the role of Data Custodian is a shared responsibility with DIT and Data Managers specified in select departments.
Data Ownership	Jackson State University is considered the data owner of all institutional data; individual units or departments may have stewardship responsibilities for portions of the data.
Data Managers	University officials who have planning and policy-level responsibilities for data in their functional areas are considered Data Managers. The Data Managers, as a group, are responsible for recommending policies, establishing procedures and guidelines for university-wide data administration activities, and training of Data Users on the proper handling of data. Data Managers, as individuals, have operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data. Data Managers are responsible for developing and applying standards for the management of University Data, for reviewing access privileges on an annual basis, and for ensuring that Data Users are appropriately informed of security obligations associated with their data access. For historical reasons — because data and the responsibility for data have traditionally been organized along functional or subject-area boundaries — the Data Managers are established according to this same subject-area organizing principle.
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.
Family Educational Rights & Privacy Act (FERPA)	Federal law (P.L. 93-568, 2) as amended in 1974 (with updates). Specifies rights and responsibilities of students and colleges regarding access to student data.

Health Insurance Portability and Accountability Act (HIPAA)	Health Insurance Portability and Accountability Act of 1996 and its implementing regulations and any updates or amendments to the same.
Information Security Officer	University official who has oversight responsibility for the University's data security program as well as compliance with relevant regulations, security policies, standards and guidelines.
Illegal File Sharing	Using file sharing applications to illegally access or share copyrighted materials
Peer to Peer File Sharing	The distribution of digital media such as software, videos, music, and images through an informal network in order to upload and download files
Protected Health Information	"Protected Health Information" or PHI is all individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law.
Qualified Machine	A "Qualified Machine" is a computing device located in a secure facility and with access control protections that meets JSU Division of Information Technology standards.
Student Records	"Student Records" are those University Data types that are required to be maintained as non-public by the Family Educational Rights and Privacy Act (FERPA). Student Records include Jackson State-held student transcripts (official and unofficial), and Jackson State-held records related to: (i) academic advising, (ii) health/disability, (iii) academic probation and/or suspension, (iv) conduct (including disciplinary actions), and (v) directory information maintained by the Registrar's Office and requested to be kept confidential by the student. Applications for student admission are not considered to be Student Records unless and until the student attends Jackson State University.
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.

4.0 Employee Adherence

The above definitions apply to all JSU employees, units and departments that need and use University data as part of their assigned duties.

5.0 Policy

6.0 Related Standards, Policies, and Processes

- IHL Policies and Bylaws, Section 1111 Digital and Electronic Copyright Infringement (November 15, 2018)
- JSU Staff Handbook, 5.5.3 Digital and Electronic Copyright Infringement Policy (DECIP) (August 2015)

7.0 Revision History

- Document Created: December 7, 2015
- Revised: February 13, 2019