Policy Name	Acceptable Use Policy
Policy Number	50000.003
Effective Date	March 29, 2019
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	March 29, 2019

1.0 Policy Statement

Jackson State University's ("JSU" or "University") Division of Information Technology's ("DIT") intention for publishing an Acceptable Use Policy is not to impose restrictions contrary to JSU's established culture of openness, trust, and integrity. DIT is committed to protecting JSU faculty, staff, students (collectively, "users"), and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems; including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, cloud integration, WWW browsing, websites, and active directory are the property of JSU.

Effective security is a team effort requiring the participation and support of every JSU user and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer systems, printers, digital devices or systems, network, email, websites, and active directory at JSU.

These rules are in place to protect its users and JSU. Inappropriate use exposes JSU to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Definitions

- 3.1 Spam: Unauthorized and/or unsolicited electronic mass mailings
- 3.2 Junk: Non-University business related email
- 3.3 Users: JSU employees (faculty, staff, students, alumni)
- 3.4 FERPA: Family Educational Rights and Privacy Act
- 3.5 Personally Identifiable: Information that can be directly tie to an individual
- 3.6 GLBA: Gramm-Leach-Bliley Act (Protection of banking information)
- 3.7 SOX: Sarabanes-Oxley Act (Integrity of financial reporting)

4.0 Employee Adherence

This policy applies to faculty, staff, students, alumni, contractors, consultants, vendors, and other workers at JSU, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by JSU.

5.0 Policy

5.1 **General Use and Ownership**

While JSU's network administration desires to provide a reasonable level of integrity, users should be aware that the data/email they create/receive on University systems remain the property of JSU and that no privacy can be expected while using these systems. Because of the need to protect the University's network, management cannot guarantee the confidentiality of information stored on any network device belonging to JSU. JSU is responsible for exercising good judgment regarding the reasonableness of personal use. DIT recommends that any information which users consider sensitive or vulnerable be password protected. For security and network maintenance purposes, authorized individuals within the DIT group may at any time analyze network utilization, traffic patterns and volumes related to JSU systems/equipment and network. JSU's DIT Group reserves the right to audit networks and systems periodically to ensure compliance with this policy.

5.1.1 Secured and Proprietary Information
(Personally Identifiable, FERPA, GLBA, SOX, Federal/State regulated. See definitions in Section 3 of this policy.)

5.1.1.1 All users should take all necessary steps to prevent unauthorized access to this information. Keep passwords secure and do not share accounts.

5.1.1.2 Authorized users are responsible for the security of their passwords and accounts.

5.1.1.3 System level passwords should be changed biannually (every 6 months). Previously used passwords will not be permissible.

5.1.1.4 User level passwords should be changed biannually every 6 months).

5.1.1.5 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (Control+Alt+Delete for Win users) (Control+Shift+Eject for Mac users) (Control+Shift+Power for Retina Macbook Pro) when the system will be unattended. Because information contained on portable computers is especially vulnerable, special care should be exercised to protect this data.

5.1.1.6 All Postings by employees from JSU email addresses to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of JSU, unless posting is in the course of business duties. Employees must use extreme caution when opening email

attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

5.2 **Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances are users of JSU authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing JSU-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

5.2.1 System and Network Activities: The following activities are strictly prohibited, without exception:

5.2.1.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by JSU.

5.2.1.2 Collection, storage or distribution of pornography or material considered to be obscene in violation of this policy.

5.2.1.3 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted movies and the installation of any copyrighted software for which JSU or the end user does not have an active license is strictly prohibited.

5.2.1.4 Illegally exporting software, technical information, encryption software or technology in violation of international or regional export control laws.

5.2.1.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.)

5.2.1.6 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5.2.1.7 Using a JSU computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

5.2.1.8 Making fraudulent offers of products, items, or services originating from any JSU account.

5.2.1.9 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, the following: Accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

5.2.1.10 Port scanning or security scanning is expressly prohibited unless prior notification is given to DIT and/or these processes are within the scope of regular duties.

5.2.1.11 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duties.

5.2.1.12 Circumventing user authentication or security of any host, network, or account.

5.2.1.13 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

5.2.1.14 Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, by any means, locally or via the Internet/Intranet/Extranet.

5.2.1.15 Providing information about (or lists of) JSU users protected/non-directory information to parties outside the University without the express written permission of the University Administration.

5.2.1.16 Any person found in violation of this policy will be notified immediately to cease and desist. The user will be given a time frame to comply or be disconnected from the JSU network until they can prove the issue has been addressed.

5.2.2 Email

5.2.2.1 The University email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any University employee should report the matter to their supervisor immediately.

5.2.2.2 Users are prohibited from forwarding JSU business email outside of JSU email system. If the user forwards emails, such message should not contain University data or information.

5.2.2.3 Users are prohibited from using third-party email systems and storage servers such as Yahoo, and MSN Hotmail, and Dropbox etc. to conduct University business or store JSU data and information.

5.2.2.4 Personal use that creates a direct cost for the University is prohibited.

5.2.2.5 Using email resources for personal monetary gain or for commercial purposes that are not directly related to University business is prohibited.

5.2.2.6 Use of email to unlawfully harass or intimidate others or to interfere with the ability of others to conduct University business.

5.2.2.7 Using a reasonable amount of University resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.

5.2.2.8 No JSU user may use his or her personal and/or third party emails to conduct official JSU business.

5.2.2.9 Sending or receiving copies of documents or files that constitute plagiarism in violation of copyright laws is prohibited.

5.2.2.10 Capture and "opening" of email except as required in order for authorized employees to diagnose and correct delivery problems or as required by law.

5.2.2.11 Use of email systems for any purpose restricted or prohibited by laws or regulations.

5.2.2.12 "Spoofing"; i.e., constructing an email communication so it appears to be from someone else in an attempt to misrepresent or hide identity.

5.2.2.13 Attempting unauthorized access to email or attempting to breach any security measures on any email system, or attempting to intercept any email transmissions without proper authorization is prohibited.

5.2.2.14 Creating or forwarding chain letters or other pyramid schemes of any type.

5.2.2.15 Running a spambot using JSU email account or resources in an attempt to send messages to large number of users or newsgroup.

5.2.2.16 Use of unsolicited email originating from within JSU's networks to advertise, any service not hosted by JSU.

5.2.2.17 Posting messages using groups account or listserv to JSU community without prior and adequate approval.

5.2.2.18 Use of faculty/staff email once it has been disabled. Faculty/Staff that are no longer employed with the university but still maintain a student status must use their student email account.

- NOTE: Please refer to the Email Policy for more information.

5.2.3 Website

5.2.3.1 Use of profanity in any form including research purposes without expressed or written consent from JSU's DIT department.

5.2.3.2 Use of any language that in any way articulates disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

5.2.3.3 Use of spyware, viruses, worms, and other malware or harmful files that compromise and shutdown university systems.

5.2.3.4 Linking to sites that display hate or pornographic images including research purposes without the expressed or written consent of the IT department.

5.2.3.5 Listing of any users' Private Personal Information (PPI). No student's PPI can be made publicly available under FERPA law.

5.2.3.6 Collection of student's PPI via forms without the written consent of the DIT department.

5.2.3.7 Any use of university website that breaches any applicable local, state, federal, or national laws or regulations.

5.2.3.8 Any use of university website that is unlawful or fraudulent, or has any unlawful or fraudulent purpose or effect.

5.2.3.9 Transmitting or procuring the sending of any unsolicited or unauthorized advertising or promotional material or any other form of similar solicitation (spam).

5.2.3.10 Sending and receiving, uploading, downloading, use or reuse of any material which does not comply with university content standards.

5.2.3.11 Knowingly transmitting any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.

5.2.4 Active Directory

Authentication

5.2.4.1 JSU users are always added automatically through Banner and should never be input ad hoc.

5.2.4.2 Vendors should be input ad hoc as needed via request and permission from DIT.

5.2.4.3 Any system attached to the domain must be JSU property identifiable by E-number or affiliated with JSU in some way (e.g., service utilization, CBORD).

5.2.4.4 Services utilizing this domain (i.e., one.jsums.edu) must maintain records/logs of interaction with AD and configuration of the system attached to the domain.

Password

5.2.4.4.1 All passwords should be reasonably complex and difficult for unauthorized people to guess. Users must choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters.

5.2.4.4.2 Users must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1" and “Pa$$w0rd” are weak from a security perspective.

5.2.4.4.3 All passwords must be changed regularly, with the frequency of every 90 days (3 months).

5.2.4.4.4 Default passwords — such as those created for new users when they start or those that protect new systems when they’re initially set up — must be changed within 24 hours.

5.2.4.4.5 Users may never share their passwords with anyone else, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

5.2.4.4.6 Users may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

5.2.4.4.7 Users should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All users will receive training on how to recognize these attacks.

5.2.4.4.8 Users must refrain from writing passwords down and keeping them at their workstations.

5.2.4.4.9 Users may not use password managers or other tools to help store and remember passwords without permission from DIT.

6.0 Policy Compliance

6.1 *Faculty, Staff, Students*

Any faculty, staff, or student found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion and/or termination of employment in accordance with procedures defined by JSU administrative policies stated in the handbook governing that individual.

6.2 *External Entities*

Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

7.0 Related Standards, Policies, and Processes

- Email Policy

8.0 Revision History

- Created: June 4, 2015
- Revised: June 8, 2015 - Added Website and Active Directory (AD) sections
- Revised: June 10, 2015 - Added AD Policies
- Revised: June 19, 2015 - Added Password Policy to AD section
- Revised: January 22, 2016 - Amended Email section of Policy
- Revised: February 13, 2019
- Revised: March 29, 2019 – Corrected the Policy Number