Policy Title: Email Policy

Policy Number: DIT-001

1) Overview

The policy has been customized to accommodate the incorporation of Google Workspace for Education Agreement and their email service to the Jackson State University (JSU) Information Technology (IT) infrastructure. Therefore, Google's Terms of Service (TOS) are also included in this document via this link: https://www.google.com/apps/intl/en/terms/education_terms.html.

Although Google's TOS is included in this document for the user's convenience, JSU does not incorporate, adopt, or necessarily agree to those terms by virtue of this policy. If any of the TOS provided via the link above is amended and in conflict with the terms of this policy, then the terms of this policy shall have priority over any conflicting terms. Additionally, any provision not permitted by Mississippi law for JSU to agree or incorporate will be considered void.

Note: All data and information created, transmitted, or stored via the JSU email systems (hosted internally or otherwise) are JSU property. Consequently, the university has taken reasonable precautions to prevent unlawful third-party access to these data.

2) Definition and Terms

As used in this policy:

a) "Data" – Includes University, student, alumni, faculty and staff data.
b) "Email"- Electronic messages distributed via a computer network to one or more recipients.
c) "Employee" – Includes JSU faculty, staff, contractors, consultants and agents.
d) "FERPA"- Family Educational Rights and Privacy Act.
e) "Information" – Includes University, student, faculty and staff information.
f) "Student" – anyone enrolled and registered for classes at JSU
g) "University"- Jackson State University.
h) "Users" – User of Jackson State University email system and electronic communication resources.

3) Purpose

Email is one of the primary modes of communication within Jackson State University, as such, the University provides email resources to support its work and mission. However, misuse and inappropriate usage can cause damage to the email system, poses legal, privacy and security risks. Thus, the purpose of the policy is to ensure security and

integrity of JSU's email system and to inform users of the importance of adherence to the guidelines provided herein.

4) Scope

This policy applies to all Jackson State University (JSU) employees, students, alumni contractors, consultants and individuals using communication technologies to transmit information or data via JSU email system or computer network. It covers software platforms, and computing devices, this means, it does not make any difference if you use JSU email on your personal device or JSU computing device. The email policy provides guidelines on appropriate usage of the University's email. These include, (a) privacy and confidentiality, (b) email address format, (c) email usage, (d) account creation/deactivation, (e) technical support, (f) university access and disclosure and (g) monitoring of communication disclosure.

5) Policy

a) Privacy and Confidentiality

Jackson State University and Google will make reasonable efforts to maintain the integrity and effective operation of its e-mail systems, but **users are advised that those systems should in no way be regarded as a secure medium for communication of sensitive or confidential information.** Due to the inherent security limitations of electronic communications, the University cannot assure the privacy of individual user's email resources nor the confidentiality of messages that may be created, transmitted, received, or stored**.**

b) Email Address Format

i. Employee email accounts use the format j-number@jsums.edu, email address aliases will have the format firstname.mi.lastname@jsums.edu or firstname.lastname@jsums.edu for users with no middle initial. Student account takes the form j-number@students.jsums.edu email address will follow the same format mentioned above, followed by the respective domain names firstname.mi.lastname@students.jsums.edu or firstname.lastname@students.jsums.edu. Alumni account will be j-number@alumni.jsums.edu and alumni email address is firstname.mi.lastname@alumni.jsums.edu or firstname.lastname@alumni.jsums.edu if no middle initial.

ii. In the case of email address conflicts, where two different users have the same exact name in the same domain, this will be resolved by appending digits at the end of the user's name. (e.g., john.doe@jsums.edu and john.doe@jsums.edu), then, using a "first-come first-served" approach, the email addresses will be john.doe@jsums.edu and john.doe1@jsums.edu, respectively.

iii. Department, University unit and organization will use service accounts, e.g., s000123456@jsums.edu. As such, the email address will have the name or acronym of the requesting unit followed by @jsums.edu. For example, physics@jsums.edu or occ@jsums.edu, or as requested by the unit's head/supervisor (Dean, V.P., Chair, etc.).

iv. Vendors, contractors and consultants will use a service account with the format v00012345@jsums.edu

v. Users will log in with JSU j-number, and University units or organizations will log in with service account s-number, e.g., j00012345@jsums.edu, j00012345@students.jsums.edu j00012345@alumni.jsums.edu, or s00012345@jsums.edu and password respectively.

vi. The default password is set to the user's date of birth (mmddyyyy), e.g., 05251985. Departments and University units with service accounts (e.g. s000123456@jsums.edu) will contact email support for a password.

c) Email Usage

1 Acceptable Use of Email

i. Only University faculty, staff, students, alumni, and other internal or external persons or organizations who have received email accounts through Information Technology (IT) are authorized users of the University's email systems and resources.

ii. JSU will use the email provided to users as an official means of communication, e.g., between faculty and students or between supervisor and employee.

iii. JSU email accounts should be used for all official email correspondence and communication. Employees must ensure to use the @jsums.edu email account for all University business, including receiving and responding to emails.

iv. University email systems and resources should be used primarily for JSU business-related purposes. Limited or occasional personal unofficial email communication is permitted provided it is lawful and bears no cost to JSU.

v. Email usage must be consistent with Jackson State University's policies and procedures of ethical conduct, safety, and compliance with applicable laws and proper business practices.

vi. All Users are allotted as much space as Gmail/Google and/or JSU IT deems necessary. Students are allotted 15GB of storage. The user has the ultimate responsibility for preserving his/her data. Email attachments are limited to 25MB for the entire message (including message and attachment), both sending and receiving. Please note that email accounts will be deactivated or deleted when a user is no longer an employee or a student of JSU. It is the user's responsibility to back-up or transfer any necessary personal information before leaving or graduating from JSU. Backing up of JSU data is prohibited.

vii. The user is responsible for ensuring that email messages and/or attachments sent or received are secure. Encrypt all confidential and sensitive messages using the encryption tools or platform provided.

2. Prohibited Use of Email

i. Jackson State University email system shall not 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, sexual harassment, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Jackson State University employee should report the matter to their supervisor immediately.

ii. Users are prohibited from forwarding JSU business email to a non-JSU email system. If the user forwards emails, such messages should not contain Jackson State University data or confidential student information.

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

iv. Personal use that creates a direct cost to the University is prohibited.

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

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

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

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

ix. Unauthorized access to other users' email by attempting to hack, breach, and subvert security measures on the JSU email system, or attempting to intercept any email transmissions without proper authorization is prohibited.

x. Creating or forwarding chain letters requesting users to forward messages or other pyramid schemes of any type.

xi. Running a spambot, phishing, spoofing, or using JSU email to send messages to a large number of users or newsgroups without prior authorization is prohibited.

xii. Sending or posting mass email messages using JSU email account, groups account or listserv to JSU community without prior and adequate approval.

xiii. Use of employee email once it has been deactivated is prohibited. Faculty/Staff that are no longer employed with the university but still maintain a student status must use their student email account.

xiv. Sending malicious messages with attachments containing viruses or malware is prohibited.

d) Account Creation/Deactivation

1. Unless denied within the University's discretion, accounts will be created for:
   i. Admitted Students for active school terms.
   ii. Currently employed Faculty or Adjunct.
   iii. Currently employed Staff.
   iv. Currently employed in Administration.
   v. Alumni.(when dues are paid to the office of Alumni relations)
   vi. Internal and external entities: vendors, contractors, consultants. and JSU organization as deemed necessary and with a prior request to and approval by JSU IT.

2. Accounts will be deleted or deactivated per the type of account and the appropriate event:
   i. JSU student email accounts are deactivated and deleted 365 days after graduation except when readmitted or enrolled within the one(1) year period.
   ii. Student admitted but never completed registration nor enrolled
   iii. Faculty, Adjunct, Staff, and Administration accounts will be deactivated immediately at resignation or termination as deemed necessary by their supervisors, Human Resources or IT.
   iv. Internal and external entities: vendors, contractors, consultants and JSU organization will be deactivated at the expiration date (determined at account creation).
   v. Retirees no longer have lifetime access to JSU email accounts.

6) Technical Support

a. The University will provide technical support for issues on JSU email accounts only. No personal accounts, such as user@yahoo.com, user@gmail.com, etc., will be provided with support.

b. The University will not provide email technical support for issues involving personal devices; e.g., cell phones, laptops, etc.

7) Access and Communication Monitoring Disclosure

General Provisions

i. Users shall have no expectation of privacy in data, files, software programs, information or any digital material stored, sent or received on the JSU email system.

ii. To the extent permitted by law, the University reserves the right to access and disclose the contents of faculty, adjunct, staff, students' retiree, and alumni emails without the user's consent. The University will do so when it believes it has a legitimate business need including, but not limited to, investigation triggered by indications of misconduct or misuse, as needed to protect health and safety, as needed to prevent interference with the academic mission, or as needed to locate substantive information required for University business that is not more readily available by some other means.

iii. Faculty, staff, and other non-student users are advised that the University's email systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.

iv. Students' email records may constitute "education records" subject to the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) a Federal law. The University may access, inspect, and disclose such records under conditions outlined in the statute.

v. Any user of the University's email system and resources utilizing encryption devices to restrict or inhibit access to his or her email must provide access to such encrypted communications when requested to do so under appropriate University authority.

8) Cybersecurity Threats and Best Practices

Users should be cybersecurity conscious and use extreme caution when using JSU email, ensuring to encrypt confidential or sensitive information when sending email. While JSU IT strives to provide reliable and secure email service to the University, absolute security or reliability of email cannot be guaranteed.

Malware

Viruses, trojans, botnets, and ransomware can be distributed via email messages. JSU email users should be careful not to open unexpected attachments in email messages from unknown or even known senders. Pay close attention to URL links, making sure it is legitimate before clicking or following the link.

a) Phishing
This is a fraudulent scam using email disguised to appear as a legitimate message from a reputable entity or person to trick a recipient into providing personal information such as login username and password, or bank account details for malicious purposes. The scammer crafts a message to lure targeted recipients to either reply to the email with the information requested or click on a link. The phishing email could appear to be from your supervisor. Call if you are unsure, and do not reply to a phishing email. Verify the source of email messages that seek confidential information or financial transactions.

b) Identity Theft
This occurs when hackers and fraudulent imposters obtain personally identifiable information(PII), such as social security numbers, driver's license numbers or credit card numbers, using phishing and malware. To protect yourself and JSU, here are some recommendations and best practices.

I. Be mindful not to fill out forms from unknown sender or sources.
II. Do not reply to spam emails, check email addresses to ensure it matches the name of the legitimate company.
III. Avoid clicking on suspicious links seeking personally identifiable information.
IV. Do not click or download suspicious attachments.
V. Never provide your username and password.
VI. Beware of emails purporting to be from your bank or dealing with money.
VII. Pay close attention to email content and grammar, often the email starts with generic greetings.
VIII. Create strong passwords and change them often and refrain from using the same password for all accounts.

c) Reporting Phishing
It is essential to report suspicious or phishing email messages immediately. To mitigate any further damage or propagation of such messages within the JSU email system, forward the suspicious message to JSU email administrator at email.admin@jsums.edu. Do not forward a suspected phishing message to another user. You may also call the email administrator at 601-979-0838 .

9) Policy Compliance

a. Compliance Measurement
The Information Technology team may be required to enforce compliance to this policy through various methods, including but not limited to, account deactivation, monitoring, Information Technology reporting tools, and internal or external audits.

b. Exceptions
The CIO, Email Administrator and Security team must approve any exception to this policy.

c. Non-Compliance/Disciplinary Action
An employee found to have violated this policy might be subject to disciplinary action, which may include suspension of email access privileges and up to termination of employment.

10) Related Standards, Policies, and Processes

- Acceptable Use Policy