JACKSONVILLE STATE UNIVERSITY

Manual of Policies and Procedures

POLICY NO.: VII:02 **DATE: April 2021**

REVIEW/REVISION DATES: April 2023

SUBJECT: Acceptable Use Policy

APPROVED: Dr. Don C. Killingsworth, Jr., President

PURPOSE

This policy outlines the acceptable use of computer equipment and the data networks at Jacksonville State University (JSU). These rules are in place to protect both the employee and JSU. Inappropriate use exposes JSU to risks including virus attacks, compromise of network systems and services, and legal issues.
This policy applies to employees, contractors, consultants, temporaries, and other workers at JSU, including all personnel affiliated with third parties. This policy applies to all equipment owned or leased by JSU.

Overview

An Acceptable Use Policy is not intended to impose restrictions contrary to JSU's established culture of openness, trust, and integrity. JSU is committed to protecting employees, students, partners, and the institution 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, WWW browsing, and FTP, are the property of JSU. These systems are to be used for business purposes in serving the interests of the University, and of our clients/customers during normal operations.

POLICY

General Use and Ownership

- JSU will maintain an approved list of technologies and devices along with the users who have access to such devices.
- JSU proprietary information stored on electronic and computing devices, whether owned or leased by JSU, the employee, or a third party, remains the sole property of JSU. JSU personnel must ensure through legal or technical means that proprietary information is protected in accordance with applicable University procedures and standards.
- JSU students and employees have a responsibility to promptly report the theft or loss of JSU issued devices and any unauthorized disclosure of JSU proprietary information to the Division of Information Technology.
- JSU personnel may access, use, or share JSU proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within JSU may monitor equipment, systems, and network traffic at any time.
- JSU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- System level and user level passwords that provide access to University restricted data or resources must comply with the Password Guidelines. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Online postings should follow the guidelines outlined in 'Social Media Policy and Guidelines' which are document in Policy V:03 of Jacksonville State University Manual of Policies and Procedures.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
- Any suspicious emails should be forwarded to phishing@jsu.edu for review.

Unacceptable Use

The following activities are in general, prohibited. Employees may be exempted from these restrictions during 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 is an employee of JSU authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing JSU-owned computing resources.

These lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

- System and Network Activities. The following activities are strictly prohibited, with no exceptions:

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

3. Accessing data, a server, or an account for any purpose other than conducting JSU business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing personal account/password to others or allowing use of the account by others, including family or other household members.
7. Using a JSU computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or other services originating from any JSU account.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee 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 for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior approval is obtained through JSU IT.
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/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Introducing honeypots, honeynets, or similar technology on the JSU network.
14. Interfering with or denying service to other users.
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, JSU employees or students to parties outside JSU without approval from Human Resources for employees and the Registrar for students.

Blogging and Social Media

For policies and guidelines related to Blogging and Social Media, please refer to ‘Social Media Policy and Guidelines’ which are document in Policy V:03 of Jacksonville State University Manual of Policies and Procedures.

Compliance Measurement

JSU will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
The Information Security Officer (ISO) and/or the Chief Information Officer (CIO) must approve any exception to the policy in advance.

Disciplinary Action
Violation of the standards, policies, and procedures presented in this policy by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions, or using poor judgment will not be accepted as excuses for noncompliance.

RESPONSIBILITY

The Vice President for Information Technology is responsible for this policy.

EVALUATION

This policy will be reviewed at least every five (5) years by the Vice President for Information Technology.