SECTION: Information Technology **Procedure 04.06.03**
AREA: Computer and Information Technology

SUBJECT: Computer Use Policy

I. PURPOSE AND SCOPE

This document outlines the responsibilities of all users of Texas Southern University computing equipment and its associated network equipment and environment. This document is written to comply with all applicable local, state and federal requirements. These directives apply to all users of Texas Southern University computing equipment and related computing networks.

II. POLICY STATEMENT

Texas Southern University provides each student, faculty and staff member with one or more computer accounts (user-Ids) that permit access to and use of the University's computer resources. Use of these resources is a privilege, not a right. When using these resources, individuals agree to abide by the policies of the University as well as any applicable federal, state and local laws. Texas Southern University reserves the right to limit, restrict or deny access to its computer resources as well as to take disciplinary and/or legal action against anyone who violates these policies and/or applicable laws.

III. POLICY PROVISIONS

A. Computer resources and data are considered valuable assets owned by Texas Southern University and the State of Texas. Computer software purchased or leased by the University is the property of the University pursuant to the software licensing agreements.

B. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime punishable under Texas statutes and federal laws.

C. University computer resources may not be transported without appropriate authorization. Access to computing resources is often restricted in accordance with the purpose to which the resource is dedicated.

D. No one may access a resource without authorization or use it for purposes beyond the scope of authorization. Never share an account, a password or other authentication device.

E. With proper safeguards, University offices and departments may conduct official business utilizing processes that establish identity by means of authentication systems approved by the appropriate office.

F. Authorized Use: Texas Southern University provides computer resources for the purpose of accomplishing tasks related to the University's mission. Computing resources may not be used for commercial or illegal activities. Students, including incoming students who have paid their fees, shall be allowed to use the University's computer resources for University-related purposes. Incidental personal use is permitted (see Section III.G.). Graduating students and students who leave the University for any reason shall have their computer accounts terminated, except that with the permission of the appropriate system administrator(s), continuing students enrolled for the coming fall semester may retain their computer account(s) during the summer.

Texas Southern University employees shall be allowed to use computer resources in accordance with this and other applicable University policies. When an employee terminates employment, his or her access to the University's computer resources shall be terminated immediately.

G. Incidental Use: Incidental computer use is defined as occasional minimal use for personal purposes that results in no additional cost to the University and does not interfere with assigned job responsibilities or violate any existing security/access rules. Incidental personal use of computing resources by employees permitted so long as such use is consistent with the University's Ethics Policy. All incidental personal use is subject to review and reasonable restrictions by the employee's supervisor and adherence to applicable University policies as well as state and federal law. Except for incidental personal use connected with approved outside employment/consulting, incidental personal use must not result in financial gain for the user or be for business purposes where the business is owned by the employee or the work is performed for another business. Personal use of University computing resources for consulting or outside employment, or which cannot be categorized as incidental, is prohibited.

H. Freedom of Expression: Censorship is inconsistent with the goals and mission of Texas Southern University. However, some computers, networks and software located on the University campus may be dedicated to specific research, teaching missions or other purposes that limit their use or access. The University shall not limit access to any information due to its content so long as it complies with applicable policy and legal standards. Forms of expression that are not protected by the First Amendment and which may be subject to censorship by the University include obscene material, child pornography, or other illegal material.

I. Privacy: Use of the University's computer systems may be subject to review or disclosure in accordance with the following:
   a. The Texas Public Information Act and other laws;
   b. Administrative review of computer use for security purposes or regarding a policy or legal compliance concern;
   c. Computer system maintenance;
   d. Audits; and
   e. As otherwise required to protect the reasonable interests of the University and other users of the computer system.

J. Anyone using the University's computer systems expressly consents to monitoring on the part of the University for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity or misuse of state resources, the evidence will be referred to appropriate officials, including law enforcement officials. In addition, all users should understand that the University is unable to guarantee the protection of electronic files, data or e-mails from unauthorized or inappropriate access.

K. Copyright laws extend to the electronic environment. Users should assume that works communicated through the computer network are subject to copyright laws unless specifically stated otherwise. The University's Copyright Policy requires the University community to follow all copyright law. Users who repeatedly infringe others' rights are subject to termination of their accounts.

L. Employees who violate the provisions of this policy shall be subject to cancellation of a user's computer account(s), suspension, involuntary dismissal, or other disciplinary action by the University in accordance with MAPP 02.05.03 – Discipline and Termination Policy. Matters involving violations of this policy may also be referred to legal and law enforcement agencies where applicable.

IV. RESPONSIBILITY OF USERS

A. Use the University computer resources responsibly, respecting the needs of other computer users and complying with laws, license agreements, and contracts.

B. Protect passwords and use of accounts and comply with requests to change passwords. Others are not permitted to use accounts or passwords. Confidential information contained on various computers shall not be shared with others except when that person is authorized to know such information.

C. Report any misuse of computer resources or violations of this Policy in writing to the Help Desk in the Office of Information Technology. Improper use of computing resources may include, but is not limited to:
   a. Breach of security - unauthorized access to computing resources or release of password or other confidential information on computer security;

b. Harmful access - creating a computer malfunction or interruption of operation alteration, damage, or destruction of data injection of a computer virus, and;
c. Invasion of privacy - reading files without authorization, and;
d. Using another employee's email account.

D. Comply with all reasonable requests and instructions from the computer system operator/administrator.

E. When communicating with others via the University computer system, ensure that communications reflect high ethical standards, mutual respect and civility.

F. Obtain and adhere to relevant network acceptable use policies, including no transmittal of chain emails or spam.

G. Use communal resources with respect for others. Disruptive mailings and print jobs, tying up work stations, and other disproportionate uses of computing facilities prevent others from using these resources.

H. Limit use of University computing accounts to the intended purpose. Use of University-owned computers (offices and computer labs) shall be limited to University-related business or incidental personal use. As defined in the TSU's Policy on Use of University Property by Employees, employees may use computing resources for personal reasons as long as that use does not result in additional costs or damage to the University and generally does not hinder the day-to-day operation of University offices and facilities. Use of computing resources for commercial purposes or personal gain is prohibited.

I. Report any incidents of harassment using University computing resources and facilities to the Help Desk. It may be harassment if:
   a. The behavior is unwelcome; and
   b. The behavior interferes with your ability, or the ability of others to work or study; and
   c. The behavior creates an intimidating, hostile, or offensive environment.

J. Web publishers are responsible for the content of the pages they publish and are expected to abide by the highest standards of quality and responsibility. These responsibilities apply to all publishers, whether they are colleges, departments, student or employee organizations, or individuals. A Web page should clearly identify the person or unit responsible for its creation and maintenance.

K. Members of the university community are encouraged to use email for University-related activities and to facilitate the efficient exchange of useful information. Access to email is a privilege and certain responsibilities accompany that privilege. Users of email are expected to be ethical and responsible in their use.

V. RESPONSIBILITIES OF SUPERVISORS

A. Supervisors shall ensure that employees within a department receive opportunities to attend training courses that help them to comply with this policy and other applicable University policies.
B. Supervisors shall promptly inform appropriate computer system administrators when employees have been terminated so that the terminated employee's access to University computer resources may be disabled.

C. Supervisors shall promptly report ongoing or serious problems regarding computer use to the Office of Information Technology.

VI. MISUSE OF COMPUTER RESOURCES

The following actions constitute misuse of the University's computer resources and are strictly prohibited for all Users:

A. Criminal and illegal acts. Texas Southern University's computer resources are not to be used in support of or for illegal activities. Any such use will be reported and dealt with by the appropriate University authorities and/or law enforcement agencies. Criminal and illegal use may include, but is not limited to, unauthorized access, intentional corruption or misuse of computer resources, theft, obscenity, and pornography.

B. Failure to comply with laws, policies, procedures, licensing agreements, and contracts that pertain to and limit the use of the University's computer resources.

C. Abuse of the University's computer resources, including but not limited to:
    a. Any act which endangers or damages specific computer software, hardware, program, network, security, or the system as a whole, whether located on campus or elsewhere on the global Internet;
    b. Creating or purposefully allowing a computer malfunction or interruption of operation;
    c. Injecting a computer virus on to the computer system;
    d. Sending a message with the intent to disrupt the University operations or the operations of outside entities, for example chain email, spam and broadcast storm;
    e. Printing materials that tie up computer resources for an unreasonable time period; and
    f. Failing to adhere to time limitations which apply at particular computer facilities on campus.

D. Use of computer resources for personal financial gain or for a personal commercial purpose.

E. Failure to protect a password or account from unauthorized use.

F. Permitting someone to use another's computer account, or using someone else's computer account.

G. Unauthorized use, access or reading of any electronic file, program, network, or the system.

H. Unauthorized use, access, duplication, disclosure, alteration, damage, or destruction of data contained on any electronic file, program, network, or University hardware or software.

I. Unauthorized duplication of commercial software. All commercial software is covered by copyright. Duplication of software protected by copyright is a violation of the law and of this policy.

J. Attempting to circumvent, assisting someone else or requesting that someone else circumvent any security measure or administrative access control that pertains to University computer resources.

K. Using the University computer system in a manner that violates other University policies such as racial, ethnic, religious, sexual or other forms of harassment.

L. Using the University's computer system for the transmission of commercial or personal advertisements, solicitations, promotions, or political material except as may be approved by the President and/or Board of Regents.

VII. AUDITOR ACCESS OF UNIVERSITY COMPUTING RESOURCES

A. In the event the University's internal auditors require access to University computer resources and data files, such access will be permitted in accordance with these guidelines.

B. Internal auditors shall:
   a. Be allowed access to all University activities, records, property, and employees as need for the performance of their duties.
   b. Notify the Chief Information Officer and the Office of General Counsel before accessing individual data files.

C. State and federal auditors shall be granted access to University computer resources and data files on an as needed basis, as approved by the President and Office of General Counsel.

VIII. RETENTION OF ELECTRONIC RECORDS

A. As a State institution, the University must maintain its records in accordance with record retention schedules filed with the Texas State Library and approved by the State Archives Commission and State Auditor's Office. These schedules apply to electronic documents in the same way they apply to paper documents. Records should be kept only so long as is necessary. Employees must familiarize themselves with the retention periods that apply to the kinds of information they create or receive. Our retention schedules give us the right to dispose of University records so it is important that we follow them and destroy our records in a systematic way.

B. Additional information regarding retention schedules may be found in MAPP 02.04.01.

IX. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

Review: Every three years, on or before September 1

X. APPROVAL

Chief Operating Officer

President

06/24/09

Date of President's Approval