TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **Policy 04.06.20**
AREA: Information Security

SUBJECT: Information Resource & Technology Privacy Policy

I. INTRODUCTION

Privacy policies are mechanisms used to establish the limits and expectations for the users of University information resources. Internal users should have no expectation of privacy with respect to information resources. External users should have the expectation of complete privacy with respect to the use of information resources except in cases of suspected wrongdoing.

II. PURPOSE & SCOPE

The purpose of the Information Resource & Technology Privacy Policy is to clearly communicate the University's information technology privacy expectations to information resource users. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Information Resource & Technology Privacy Policy applies equally to all individuals who use any University information resource.

III. OWNERSHIP

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of the University are the property of the University and the State of Texas.

IV. POLICY PROVISIONS

A. Electronic files created, sent, received, or stored on owned, leased, administered, or otherwise under the custody and control of the University are not private and may be accessed by the Office of Internal Audit and OIT at any time without knowledge of or notice to the information resource user or owner.

B. To manage systems and enforce security, the University may log, review, and otherwise utilize any information stored on or passing through its information resource systems in accordance with the provisions and safeguards provided in TAC 202, Information

Resource Standards, TSU Security and Technical Monitoring Policies. For these same purposes, the University may also capture User activity, such as telephone numbers dialed and web sites visited.

C. A wide variety of third parties have entrusted their information to the University for business purposes, and all workers at the University must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; accordingly, customer account data is confidential and access will be strictly limited based on business need for access.

D. Users must report any weaknesses in University computer security or any incidents of possible misuse or violation of this agreement to the Information Security Officer.

E. Users must not attempt to access any data or programs contained on University systems for which they do not have authorization or explicit consent.

V. PUBLIC ACCESS PRIVACY POLICY STATEMENT

The University's web site must contain the following Privacy Statement:

Web site privacy statement on the use of information gathered from the general public

The following statement applies only to members of the general public and is intended to address concerns about the types of information gathered from the public, if any, and how that information is used.

1. COOKIES

A —cookie is a small file containing information that is placed on a user's computer by a web server. Typically, these files are used to enhance the user's experience of the site, to help users move between pages in a database, or to customize information for a user. Any information that university web servers may store in cookies is used for internal purposes only. Cookie data is not used in any way that would disclose personally identifiable information to outside parties unless the university is legally required to do so in connection with law enforcement investigations or other legal proceedings.

2. LOGS AND NETWORK MONITORING

The university maintains log files of all access to its site and also monitors network traffic for the purposes of site management. This information is used to help diagnose problems with the server and to carry out other administrative tasks. Log analysis tools are also used to create summary statistics to determine which information is of most interest to users, to identify system problem areas, or to help determine technical requirements. Information such as the following

is collected in these files:

A. *Hostname: the hostname and/or IP address of the computer requesting access to the site.*
B. *User-agent: the type of browser, its version, and the operating system of the computer requesting access*
C. *Referrer: the web page the user came from.*
D. *System date: the date and time on the server at the time of access*
E. *Full request: the exact request the user made*
F. *Status: the status code the server returned, e.g., fulfilled request, file not found.*
G. *Content length: the size, in bytes, of the file sent to the user.*
H. *Method: the request method used by the browser (e.g., post, get)*
I. *Universal resource identifier (uri): the location of the particular resource requested (more commonly known as a uri).*
J. *Query string of the uri: anything after a question mark in a uri. For example, if a keyword*
Search has been requested, the search word will appear in the query string.
K. *Protocol: the technical protocol and version used, i.e., http 1.0, ftp, etc.*

The above information is not used in any way that would reveal personally identifying information to outside parties unless the university is legally required to do so in connection with law enforcement investigations or other legal proceedings.

3. EMAIL AND FORM INFORMATION
If a member of the general public sends the university an e-mail message or fills out a web-based form with a question or comment that contains personally identifying information, that information will only be used to respond to the request and analyze trends. The message may be redirected to another government agency or person who is better able to answer your question. Such information is not used in any way that would reveal personally identifying information to outside parties unless system administration is legally required to do so in connection with law enforcement investigations or other legal proceedings.

4. LINKS
This site may contain links to other sites. The university is not responsible for the privacy practices or the content of such websites.

5. SECURITY
This site has security measures in place to protect from loss, misuse and alteration of the information

VI. DISCIPLINARY ACTION

Violation of this policy may result in immediate Disciplinary Action pursuant to University policy (MAPP 02.05.03 – Discipline and Termination Policy).

VII. APPLICABLE TSU SECURITY POLICY STANDARDS

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 2
- Security Standard 3
- Security Standard 16

VIII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer Billy Ratcliff

Review: Every year, on or before September 1

IX. APPROVAL

Jimi McShan
Vice President of Finance

Joe Ridley
President

2/18/11
Effective Date