TEXAS SOUTHERN UNIVERSITY

MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **NUMBER: 04.06.05**
AREA: Computer and Information Technology

TITLE/SUBJECT: Acquisition Assessment Policy

I. POLICY STATEMENT

The Acquisition Assessment Policy has been put in place to ensure the confidentiality, integrity, and availability of Texas Southern University's Information Resources. Acquiring new technology can have a negative impact on the University's Information Resources if not properly assessed by the Office of Information Technology and the Information Security Team.

II. PURPOSE AND SCOPE

The purpose of the Acquisition Assessment Policy is to define the process to deal with academic or administrative departments that wish to acquire software/hardware. Acquired systems connect to the university network, interface with university systems, or require centralized support. To the extent this policy conflicts with an existing University policy, the existing policy is superseded. All University employees must comply with the provisions of this policy as well as the provisions of the related Software License Policy – MAPP 04.06.02.

III. DEFINITIONS

N/A

IV. POLICY PROVISIONS

1. The Information Security Team must be engaged to perform appropriate Risk Analysis and/or Business Impact Analysis.

2. Prior to purchasing any software/hardware systems the department will contact the Office of Information Technology (OIT).

3. OIT must evaluate the software/hardware to determine its resource requirements and interface to existing University systems, security concerns and vulnerabilities, any internal costs for programming, systems administration, training, networking or other support requirements. OIT must also evaluate to ensure there are not already existing University software/hardware systems that provide equivalent functions.

4. The appropriate OIT representative will conduct an evaluation of the desired system with the department and vendor, and will provide the department with an assessment report detailing all of the aspects of the evaluation.

5. The department will then have all of the necessary information to make an informed decision as to whether they want to acquire the system. Any risks associated with the purchase of the new software/hardware must be accepted by the CIO and the department acquiring the software/hardware system.

6. OIT will only support systems that have followed the proper acquisition assessment process.

7. Disciplinary Action

   Violation of this policy may result in immediate disciplinary action pursuant to University policy (MAPP 02.05.03 – Discipline & Termination Policy).

8. 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 3
   - Security Standard 6
   - Security Standard 21
   - Security Standard 22

9. Review and Responsibilities

   Responsible Party: Chief Information Officer

   Review: Every 3 years, on or before September 1st

Forms

None

V. APPROVALS

Chief Information Officer

President

Effective Date 2/1/2018