## I. POLICY STATEMENT

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks/computers, improving user security awareness, and early detection and mitigation of security incidents, are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

## II. PURPOSE AND SCOPE

The purpose of the System Development Policy is to describe the requirements for developing and/or implementing new software for Information Resources. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The System Development Policy applies equally to all individuals who use any University Information Resources.

## III. DEFINITIONS

N/A

## IV. POLICY PROVISIONS

1. The Office of Information Technology ("OIT") is responsible for developing, maintaining, and participating in a System Development Life Cycle ("SDLC") for system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and postimplementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical University information.

2. All production systems must have designated Owners and Custodians for the critical information they process. The Information Security Officer must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

3. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular user on the system in question) must be assigned for all production systems.

4. Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system while the development and test environments can maximize productivity

with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.

5. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

6. Disciplinary Action

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

7. 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 8
- Security Standard 10
- Security Standard 11
- Security Standard 14
- Security Standard 17