SECTION: Information Technology   **NUMBER:** 04.06.09
AREA: Computer and Information Technology

TITLE/SUBJECT: Computer Virus Detection Policy

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 and computers, improving user security awareness, and early detection and mitigation of security incidents can reduce the risk and drive down the cost of security incidents.

II.   PURPOSE AND SCOPE

The purpose of the Computer Virus Detection Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

The Computer Virus Detection Policy applies equally to all individuals who use any University information resource.

III.   DEFINITIONS

N/A

IV.   POLICY PROVISIONS

1. All workstations, whether connected to the University network or standalone, must use Office of Information Technology ("OIT") approved virus protection software and configuration.

2. The virus protection software on a computer must never be disabled or bypassed.

3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

4. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates or disabled to prevent updates.

5. Each file server attached to the University network must utilize OIT approved virus protection software and setup to detect and clean viruses that may infect file shares.

6. Each e-mail gateway must utilize OIT approved e-mail virus protection software and must adhere to OIT rules for the setup and use of this software.

7. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the OIT Help Desk.

8. Disciplinary Action

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

9. 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 1
    - Security Standard 3
    - Security Standard 6
    - Security Standard 7
    - Security Standard 16
    - Security Standard 21
    - Security Standard 22

10. Review and Responsibilities

    Responsible Party: Chief Information Officer

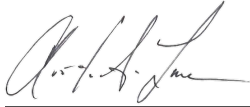   Review: Every 3 years, on or before September 1st

Forms

    None

V.   APPROVALS

_____
Chief Information Officer

_____
President

Effective Date   _____ 2/1/2018 _____