TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **Policy 04.06.09**
AREA: Information Security

SUBJECT: Computer Virus Detection Policy

I. INTRODUCTION

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

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 To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

III. SCOPE

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

IV. POLICY

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

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

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

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

E. 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.

F. 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.

G. 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.

V. DISCIPLINARY ACTION

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

VI. 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

VII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer Billy Rath

Review: Every year, on or before September 1

VIII. APPROVAL

Jimi McShan
Vice President of Finance

John Ruckley
President

2/18/11
Effective Date