SOUTHERN UNIVERSITY A&M
Agricultural & Mechanical College

ANTIVIRUS POLICY

March 2008
Updated April 2019

TNS –POL - 012

PURPOSE

Southern University shall promote a secure computing environment for all students, faculty, staff and affiliates. Computing platforms (including but not limited to: desktop workstations, laptops, hand-held, personal digital assistants, servers and network devices) are integral elements in the operations of the University and as such are vital to the University's mission. This policy will help ensure that all vulnerable computing platforms on campus are guarded against vulnerabilities and protected by antivirus software at all times.

SCOPE

This document describes the measures taken by the University to counter computer viruses and identifies the responsibilities of individuals, departments and Division of Information Technology in protecting the University against viruses and other vulnerabilities.

OBJECTIVES

The principal concern of this computer virus protection policy is effective and efficient prevention of all network virus outbreaks and network security attacks involving all computers associated with Southern University. The primary focus is to ensure that Southern University-affiliated users (faculty, staff, and students) are aware of and take responsibility for the proper use of the University-provided and Division of Information Technology supported virus protection software. This policy is intended to ensure:

1. the integrity, reliability, and good performance of University computing resources;
2. that the resource-user community operates according to a minimum of safe computing practices;
3. that the University licensed virus software is used for its intended purposes; and
4. that appropriate measures are in place to reasonably assure that this policy is honored.

POLICY STATEMENT

Any computer, server or network devices connected to the Southern University network shall be protected by antivirus software from malicious electronic intrusion. This policy applies to all devices connected, by any means, to the Southern University network including those owned by the University, private individuals such as faculty, staff and students, affiliates, and third-party vendors.

All computers or networked devices shall have applicable operating system and application security patches and updates installed prior to initial connection to the network. Additionally, those personal use systems for which antivirus software is available shall have it installed and configured for effective operation prior to their connection to the campus network.

DoIT is solely responsible for the purchase of antivirus software for all Southern University computers, servers, or any network device connected to the Southern University network. Other departments are **prohibited** of purchasing any antivirus software for any University computer systems, unless given permission by DoIT.

DIVISION OF INFORMATION TECHNOLOGIES RESPONSIBILITIES

Obligation and Usage

DoIT purchases antivirus software and licenses for all computer systems.

- Installation of the antivirus software is required on ALL university owned machines on the campus. This product is provided to all university computers, servers, and network devices. Product is configured to automatically receive virus definition updates from a centralized-managed server.
- Deployment of anti-virus software.
- DoIT staff installed the antivirus software on the images used for all faculty, staff and lab computers. The software is available for all computers running on the network.
- Updating of software.
- DoIT will keep the anti-virus products it provides up to date. We utilize the antivirus software with centralized policy management. This allows us to automatically deploy new virus definitions to workstations connected to the domain.
- Centrally-managed virus protection software provided by DoIT will run on all Southern University computers, servers, or any network device connected to the Southern University network.

Containment of Virus incidents

- DoIT staff will take appropriate action to contain virus infections and assist in their removal. In order to prevent the spread of a virus, or to contain damage being caused by a virus, DoIT may remove a suspect computer from the network or disconnect a segment of the network.
- DoIT will provide advice to individuals on the function and installation of the anti-virus products and on virus protection. This includes advice on virus hoaxes, including occasional circulars on specific hoaxes.
- DoIT will assist individuals with recovery from viruses. This includes advice on containment to stop the spread, help with removing viruses, taking note of information about the incident and advice on how to prevent a recurrence.

Support for End-User Computers

This virus protection policy includes all operating systems. DoIT will give priority support for client computers running Windows-based operating systems. Individuals who use operating systems other than Windows-based will need to contact DoIT for supported anti-virus software for their particular operating system.

Plans

Antivirus software provided by DoIT will continue to be installed on university owned machines with virus definitions being pushed out to the managed machines.

DEPARTMENTAL RESPONSIBILITIES

- Departments with dedicated technology personnel that manage their own computers (including labs) are responsible for virus protection on computers that are within their department. This includes making sure that all computers have antivirus software installed, removing any viruses found and applying any updates necessary to defend against possible threats.
- All departmentally managed computers (including all labs) **must** use the antivirus software provided by DoIT. Tech personnel may be advised and assisted by DoIT.
- Departments managing their own servers **must** use the antivirus software provided by DoIT.
- Departments are **not** to purchase their own antivirus software, unless given permission by DoIT.

INDIVIDUAL RESPONSIBILITIES

- All administrators, faculty, staff and students are responsible for taking suitable measures to protect against virus infection and failure to do so may constitute an infringement of this policy. A user who allows their computer to become infected puts their own work and other people's computers and data within the University and beyond at risk.
- Administrators, faculty and staff must have antivirus software installed and ensure that it is working.
    - If you are not sure if your computer system has the latest or updated antivirus software, you should contact DoIT.
- University personnel or students who are authorized to connect personal computers to the University network must ensure that computers have updated virus protection.
- Students are responsible for the virus protection for their personal computers.

Virus Protection at Home

It's recommended that in addition to the above, it is best practice to:

- Have a antivirus software installed on all computer systems
- Update virus protection software frequently (recommend automatic setup).
- Install any recommended security patches for the operating system and applications that are in use.