ELIZABETH CITY STATE UNIVERSITY
Anti-Virus, Viruses and Hoaxes Policy

I. Purpose

This guideline describes the methods and activities relating to Elizabeth City State University Information Technology security monitoring for viruses and the use of anti-virus methods. It also describes actions taken after viruses and other malicious software is detected.

The policy also includes an active program for anti-virus use and malicious software monitoring. The goal is to ensure information resource security controls are in place, are effective, and are being enforced through regular monitoring and appropriate incident response actions.

II. Scope

This policy applies to all personnel who include full time regular, temporary and part-time employees, full-time and part-time students, contractors, and all other authorized users of any University Information Systems, including University-hosted, third-party hosted, and Internet Service Providers (ISP).

III. Policy

A. Users are encouraged to make full use of the University's computing and communication resources in pursuit of legitimate activities that further the educational, research, administrative, and service mission of the institution. However, users must also be aware of the fact that there are imminent and severe threats associated with sharing files with others and with access to both the campus network and Internet. Because of the level of threat associated with this level of networked community participation, users have certain responsibilities that include the following:

1. Protecting themselves, their colleagues, and the University community through virus protection software;

2. Maintaining Virus definitions associated with the software at current levels as provided for by the manufacturer of that product;

3. Refraining from downloading, transporting, posting, transmitting, or launching material such as a computer virus, worm, Trojan Horse, or similar damaging rogue entity that is illegal or damaging to a university computing or communication;

4. Refraining from disseminating or conveying to other users hoaxes or other false information concerning viruses or similar threats.

B. ECSU may utilize a number of automated tools (e.g. Antivirus Software, Port Sentry, Sniffer, etc.) to detect threats and vulnerability exploitation, and to combat virus attacks. ECSU may monitor:

1. Internet traffic
2. Email traffic
3. LAN traffic
4. Firewall traffic
5. Desktop and Server Processes
6. Any other network or computer activities

C. Users should contact the Division of Information Technology helpdesk at helpdesk@ecsu.edu for information concerning viruses and necessary practices for ensuring protection against those viruses and similar threats.

D. Any user who believes they have information concerning the creation, propagation or dissemination of viruses or similar threats, including hoaxes, should inform the Information Technology Security Officer at itsecurityadmin@ecsu.edu or the Division of Information Technology helpdesk at helpdesk@ecsu.edu.

E. If your computer is infected with a virus:

1. Immediately unplug the network cable or disable the wireless connection.

2. Immediately call the Division of Information Technology Help Desk for assistance.

3. Be aware that viruses and worms may be transmitted through email, network connections, and removable disks, such as DVDs, CDs, floppy disks, and USB drives. Even with the advanced Antivirus Software available today, sometimes an infection may destroy the contents of a hard drive, wiping out weeks or months of work. This underscores the importance of backing up your files regularly, and keeping your data on a server drive at all times, where it is backed up daily.

F. ECSU Division of Information Technology staff cannot be held responsible for the loss of data stored on a local hard drive. Network drives are made available and their use is encouraged to avoid data loss.

G. Division of Information Technology helpdesk reserves the right to restrict access to the campus network or computing resources to ensure prevention and containment of such entities. Division of Information Technology helpdesk also reserves the right to digitally scan, by appropriate protection software, all messages and files stored on or transmitted through campus electronic resources for the presence of threats such as viruses, and to eliminate those messages and files found to contain them to ensure protection of systems, data, and other users.