07.100.10 VIRUSES AND HOAXES

Authority: Board of Trustees

History: Reformatted May 25, 2005; approved by Board of Trustees October 28, 2004; revised October 23, 2003; effective January 18, 2002

Source of Authority: Consolidated University of North Carolina Netstudy – Security Subcommittee Baseline Recommendations (Feb. 16, 2003); International Standard ISO17799

Related Links: Administrative Provisions,

Responsible Office: Information Technology Systems Division

I. Purpose

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. Users should contact the ITSD Technology Assistance Center or their local IT computing consultants for information concerning viruses and necessary practices for ensuring protection against those viruses and similar threats. Any user who believes they have information concerning the

creation, propagation or dissemination of viruses or similar threats, including hoaxes, should inform the ITSD Technology Assistance Center immediately. ITSD reserves the right to restrict access to the campus network or computing resources to ensure prevention and containment of such entities. ITSD 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.