Security Extension to Acceptable Use Policy

1.0 Purpose

Clark University must provide a secure network for our instructional, research, and administrative activities. An unsecured computer on the University network allows viruses, worms, and other attacks and compromises to enter the network, thereby affecting many computers, as well as the network's integrity. Damage from these exploits can include the loss of sensitive and confidential data, interruption of network services, and destruction of critical Clark University systems. Universities that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers or other devices (hereinafter referred to generically as "devices") to the Clark University network (hereinafter referred to as "our network") must follow specific standards and take specific actions. The purpose of this Security Extension to the Policy on Acceptable Use of Clark's Information Technology System is to define the policy governing connecting devices to the network. The policy is designed to minimize the potential exposure to Clark University and our community from damages that could result from devices that are not properly configured or maintained.

2.0 Scope

This policy applies to all members of Clark University who have any device connected to our network, including, but not limited to, desktop computers, laptop computers, server computers, wireless computers, specialized equipment, cameras, building and environmental controls. The policy applies to university-owned devices as well as personally-owned devices that connect to our network.

3.0 Policy

3.1 Appropriate Connection Methods

You may connect devices to our network at appropriate connectivity points; data jacks, and through a University operated or approved wireless network access point. You may not extend or modify our network. You may not install hardware devices such as, but not limited to, bridges, switches, wireless access points, or hubs without explicit permission from ITS Networking.

3.2 Responsibility for Security

Every device connected to our network has an associated caretaker (e.g., a faculty or staff member who has a university-owned computer in his/her office) or owner (e.g., anyone who connects a personally-owned computer to our network).

Each caretaker and owner is responsible for ensuring that his/her device meets relevant security standards and for managing the security of the device and its associated software. ITS distributes the document, Securing your Computer, detailing current

security standards, guidelines and instructions to all faculty, students and staff. This document also describes how ITS helps both caretakers and owners keep their systems secure.

Individuals who can risk no disruption in the operation of a device are strongly encouraged not to connect it to our network, or to make arrangements with ITS Networking for a local and private connection (i.e., no Internet and campus-wide network access). An example of such a device is a computer continuously collecting/analyzing data for research purposes.

3.3 Network Registration

Users of our network may be required to authenticate when connecting a device. ITS maintains a database of unique device identification, network address and caretaker/owner for contacting the caretaker/owner when necessary. For example, ITS would contact a caretaker/owner if his or her computer was putting harmful traffic on our network.

3.4 Network Analysis and Protection

By connecting a device to our network, you acknowledge that ITS routinely analyzes the behavior of network traffic and interrogates the status of devices in order to ensure a safe computing environment. Should a device exhibit any of the following characteristics, ITS will take appropriate steps to protect our network and the devices connected to it; in all cases, a good faith attempt will be made to notify the caretaker/owner:

- imposing an exceptional load on a campus service;
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others;
- exhibiting behavior consistent with compromise by a virus or other known attack.

3.5 Restricted Traffic

In order to protect our network, ITS reserves the right to restrict certain types of traffic coming into and across it.

3.6 Remote Access to Our Network

Most Clark faculty, staff and students who live off campus choose to personally contract for the services of an Internet Service Provider (ISP) in order to access the Internet from a device at their place of residence. Within possible limitations of section 3.5, faculty, students and staff may use their ISP connection to access Clark University email and Web servers. Individuals who seek to use their ISP connection to access an on-campus device -- of which they are the caretaker/owner -- from an off-campus device, must:

- Stipulate in writing that they, and only they, can and will use the off-campus device to access the on-campus device;
- Use remote control software from an approved list, and with an approved configuration, by the ITS Help Desk.

Due to very significant security risks, use of any VPN (Virtual Private Network) or

equivalent software, other than the ITS provided VPN, to directly connect an off-campus device to our network is prohibited.