Policy on Connecting Devices to the Network

Purpose

The Stephen M. Ross School of Business at the University of Michigan (“Ross”) has expended great effort to create a high-performance network environment that is robust, secure and convenient for all members of the community. A computer network is a shared resource in any organization. Decisions about how best to administer and extend network services need to be based on the needs of the entire community. As more consumer devices become network aware, such as wireless printers, dual-mode cell phones, portable media and others as they evolve, they have the potential to disrupt and degrade a computer network. This policy defines the types of devices members of the Ross community can connect to the network.

Special Considerations for Wireless Networking

Wireless networks make use of a limited number of radio frequencies or “channels.” The placement of wireless antennae and the turning of these channels is very precise. Unlike wired networks where more switches can be designed into the network, more fiber cabling run to increase performance, or more network jacks installed to accommodate more devices, radio channels cannot be added to accommodate more wireless devices. Other non-computing devices, like microwaves, can operate on these same channels causing interference and degrading performance. For these reasons, attaching wireless devices to the Ross network is never permissible.

Types of Networked Devices Prohibited

The following types of devices are prohibited:

- Any device that attempts to intercept or redirect traffic from another device on the network.
- Devices acting as a wireless base station. These devices may include, but are not limited to, access points, wireless routers, repeaters, bridges, or hotspots.
- Any device that attempts to jam, block, or in any way degrade the wireless network.
- Any device that attempts to create a bridge between different networks.
- Any device that interferes with a service provided by Ross Computing Services (for example, a DHCP server).

Remediation Steps

If a device is found to be in violation of this policy, Computing Services reserves the right to perform any or all of the following remediation actions:

- The device may be immediately disconnected from the network or blocked from further connection. An attempt will be made to notify the owner of the device.
- Unauthorized wireless base stations may be remotely contained such that clients will not be able to connect to them.

Repeated violations of this policy may result in referral to Ross or University of Michigan authorities for further action.