

THE  
**LeMoyné-Owen**  
 COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

<b>SUBJECT:</b>  Connection to Network	<b>Effective Date:</b> July 1, 2011	<b>Policy Number:</b> 05-1-002
	<b>Supersedes:</b> Policy: Date:	<b>Page</b> 1 <b>Of</b> 2
	<b>Responsible Authority:</b> Director of Information Technology	

**I. Purpose of the policy/Policy statement**

The purpose of this policy is to maintain the integrity of the Network infrastructure without interruption and disruption

All devices with a network interface that are attached to the network (including printers, computer systems, laboratory equipment, scanners, communications devices, etc.) must be registered with IT and attached to the network by IT staff. When a device is registered, network name and numbers will be assigned to the device and owner contact information will be collected

**II. Applicability/Scope**

This policy applies to all members of the College: employees and students

### III. Process for Implementing Procedure

Responsibility	Action	Timeline
Users	All users are required to contact the Help Desk before using a new or unfamiliar network program, device, or protocol. The Help Desk can determine if the item in question is compatible with the infrastructure in advance, preventing problems before they occur.	On-going
Users	Programs that cause excessive broadcast levels are forbidden: Routers, switches, firewalls, bridges, repeaters, and the protocols used by such devices may not be used on the network without specific permission from IT.	On-going
Users	Connecting devices to the network for the purpose of providing remote access is not permitted. For example, connecting a modem to an office computer so that one can access the network from one's home computer is not permitted. The connection of such a device requires the written permission of the Director of IT. Such devices present a security and operational threat to the network and a possible violation of The LeMoyne-Owen College license agreements. If such a mechanism is discovered, the device or computer will be disconnected. The only permitted mechanisms for remotely accessing the network are those provided through IT	On-going
IT Staff	Monitors the integrity of the Network	On-going

### IV. Related policies/References for more information

Authorizing Official: <u>Shirley Hill</u>	Authorization Date: <u>10/10/11</u>
Title: <u>Director of Title III</u>	