**Middlesex County College Security Policy**

The purpose of this security policy is to ensure to protect users’ information and at the same time set rules for expected behavior, authorize security personal to monitor usage and define consequences of violations of these rules therefore helping minimize risks and complying with regulations and legislation.

The Security Policy is divided in the following sub policies:

**Privacy Policy:** All users of MCC resources may be monitored and although information is not disclosed, user must know that all information stored in the college servers is property of the college.

**Acceptable Use Policy:** College resources are available to all users and their use depends on the location of the computers being use, open computer rooms are available for students who required a pc for any reason (printing, web surfing, etc), while computers labs are restricted only for the use of students on homework or projects requiring specific software (Linux, Java, VB, etc).

**Authentication Policy:** Users using any college resource must provide a valid and updated MCC ID. In case of special software (Linux OS) the user is provided with logon name and password.

**Internet Use Policy:** Improper uses of internet resources are:

* Using the Internet connection to perform any act that may be construed as illegal or unethical, including attempting to gain unauthorized access to the network.
* To insure the best overall network performance, network traffic will be monitored, if in the course of monitoring network traffic, information which may have adverse legal implications for the College is discovered, it will be reported.
* Both personal and commercial advertising must not be posted on Lee College web sites.
* Users shall not engage in activities that relate to material involving the sexual exploitation of minors as defined by Federal Code Title 18, Part I, Chapter 110, Sexual Exploitation and other abuse of children or other criminal acts.

**Access Policy:** User at allow to access the network resources on site only when the college is open, for offsite network use the user must provide a valid username and password

**Auditing Policy:** The college network has installed software to track traffic and use of resources to make sure users comply with policies, plans, procedures, laws and regulations. In case of any violation disciplinary measures will be taken.

**Data Protection Policy:** Backups are made in a daily basis; backups are made at night when fewer users are in the network. The network is protected 24/7 with antivirus antispyware, malware protection and a strict firewall. Since all data is backup, in case of any disaster all the data could be easily restored.