NETWORK COMPUTING POLICY

This Organization is responsible for securing its network and computing systems in a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action in the form of temporary revocation of user accounts, regardless of the success or failure of the attempt. Permanent revocations can result from disciplinary actions taken by a panel judiciary board called upon to investigate network abuses.

The users of the network are responsible for respecting and adhering to local, state, federal and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities. If such an event should occur, this organization will fully comply with the authorities to provide any information necessary for the litigation process.

SECTION 1: GENERAL COMPUTING POLICY

Once a user receives a userID to be used to access the network and computer systems on that network, they are solely responsible for all actions taken while using that userID. Therefore:

1.1 Applying for an userid under false pretenses is a punishable disciplinary offense.
1.2 Sharing your userid with any other person is prohibited. In the result that you do share your userid with another person, you will be solely responsible for the actions that other person appropriated.
1.3 Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
1.4 Attempts to evade or change resource quotas are prohibited.
1.5 Continued impedance of other users through mass consumption of system resources, after receipt of a request to cease such activity, is prohibited.
1.6 Use of facilities and/or services for commercial purposes is prohibited.
1.7 Any unauthorized, deliberate action which damages or disrupts a computing system, alters it normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

SECTION 2: ELECTRONIC MAIL POLICY

Whenever you send electronic mail, your name and userid are included in each mail message. You are responsible for all electronic mail originating from your userid. Therefore:

2.1 Forgery (or attempted forgery) of electronic mail messages is prohibited.
2.2 Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
2.3 Attempts at sending harassing, obscene and/or other threatening email to another user is prohibited.
2.4 Attempts at sending unsolicited junk mail, "for-profit" messages or chain letters is prohibited.

SECTION 3: NETWORK SECURITY

As a user of the network, you may be allowed to access other networks (and/or the computer systems attached to those networks). Therefore:

3.1 Use of systems and/or networks in attempts to gain unauthorized access to remote systems is prohibited.
3.2 Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote system/local, is prohibited.
3.3 Decryption of system or user passwords is prohibited.
3.4 The copying of system files is prohibited.
3.5 The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.
3.6 Intentional attempts to "crash" Network systems or programs are punishable disciplinary offenses.
3.7 Any attempts to secure a higher level of privilege on Network systems are punishable disciplinary offenses.
3.8 The willful introduction of computer "viruses" or other disruptive/destructive programs into the organization network or into external networks is prohibited.

_____ _____ _____

Signature Date UserID

by Wes Morgan (morgan@engr.uky.edu) and Arlene H. Rinaldi (rinaldi@acc.fau.edu)

Permission to duplicate or distribute this document is granted with the provision that the document remains intact or if used in pieces, that the original document source be referenced. For additions, comments, suggestions and requests for revisions, please send Email to RINALDI@ACC.FAU.EDU.