I.2. Acceptable Use of FM Information Systems and Technology

Approved by the AVP on October 24, 2000   (Revised November 14, 2002)

This policy establishes the requirements for proper use of FM computers and system resources.

1. Purpose

The purpose of this policy is to ensure that FM computers, which are a tool to perform work at the University, are maintained in a reliable efficient condition to perform these duties. This policy supplements the University’s “Guidelines for Acceptable Use of Computer Resources” (available online at http://www.umd.edu/aug). Questions about the University’s Guidelines should be addressed to Project NEThics in the Office of Information Technology at x58787 or NEThics@umail.umd.edu.

2. Responsibility

Facilities Management’s Information Technology Services (ITS) unit is responsible for keeping FM computers running and configured properly. The Assistant Director of ITS has overall responsibility for FM’s information systems and technology, and the guidelines for their proper use.

3. Ownership

FM information systems and technology include all hardware (computers and peripherals), software (applications), the FM local area network (LAN) and networked systems (WMS, PMIS, etc.).

Facilities Management’s computers and computer systems are the property of the University of Maryland. All computer systems and information stored within such computer systems are also the property of the University and may be monitored. Anyone using these systems expressly consents to this monitoring. Information may also be subject to disclosure under the Maryland Public Information Act or by court order.

4. Access

Access to the Management Information System and local area network is provided to authorized users only. Accounts issued to individuals are for the sole use of that individual and are non-transferable. The owner is responsible for all usage on that account. Unauthorized access to FM's local area network, files or computers is in violation of Article 27 Sections 45A and 146 of the Annotated Code of Maryland and may result in prosecution or disciplinary action.

5. Software

All software licenses purchased by Facilities Management are the property of Facilities Management and the University of Maryland, College Park. Software is not to be copied for personal use, except as permitted by software licensing agreements.

U.S. copyright laws and international treaty provisions protect all licensed software. Therefore, you must treat the software like any other copyrighted material.

*Shareware* is copyrighted software that the developer allows you to copy and distribute to others. In many cases, you are obligated to pay a fee if you continue to use this software after a certain period of time. *Freeware* is software available for downloading from the Internet at no cost.

**Personal software is not allowed on University computers** except in rare job-related instances. If you wish to install any software, including commercial software, shareware or freeware, you must obtain written permission from the Manager of Network Operations or the Assistant Director for Information Technology. ITS does not provide technical support of personal software.
6. **General User Guidelines**

Users should log off of the network at the end of each day and should lock their computers or logout of secure applications when away from their desk. Users can lock their workstations in Windows NT or Windows 2000 by pressing the Ctrl-Alt-Delete key sequence and select Lock Workstation from the dialog box. If users do not log off, they will be held responsible for unauthorized use of their account.

Users should store important files on the network drives where files are backed up daily. Important files include any data or work product that you can’t afford to lose.

All individual user passwords must be kept confidential. Users should not share their password with any other user. Users are also advised to select their passwords carefully (e.g., avoid using names or common dictionary terms) and change them often. The best password is a combination of letters, numbers, and symbols.

7. **Expressly Prohibited Activities**

There are certain activities that are not permitted except by authorized ITS personnel and may result in disciplinary action. These include, but are not limited to:

- Purchasing any computer hardware or software using University money except for building-specific equipment (CCMS, Alarms, etc).
- Installing any software on any FM workstation
- Sending email from someone else’s account without proper authorization
- Adding, removing or substituting any hardware components in FM workstations
- Opening the computers for any purpose
- Altering or accessing any files without proper authorization
- Malicious damage of computer equipment
- Relocation or removal of computer equipment without proper authorization from Network Operations or the Assistant Director for Information Technology Services.
- Operating a business using University equipment.

8. **Compliance**

FM’s Network Operations Manager and support staff have the responsibility to report any infractions of this policy. Violations of this policy may result in disciplinary action, removal of network access, or legal action. Questions about this policy can be directed to the Assistant Director of Information Technology Services or Manager of Network Operations.

9. **User Acceptance of Agreement**

All employees using FM computer resources must sign an FM ITS agreement acknowledging their understanding of this policy and willingness to comply with its guidelines. Electronic signatures will be retained by network manager; hard copies will be kept by Human Resources in personnel files.
10. Policy Review

This policy will remain in effect until it is revised due to substantive organizational or operational changes or if the University’s policy changes.

Asst. Vice President, Facilities Management
Effective Date: October 24, 2000 (Revised: November 14, 2002)