

# MANUAL OF PROCEDURE

---

|                             |  |                    |
|-----------------------------|--|--------------------|
| <b>PROCEDURE NUMBER:</b>    | 7900   | <b>PAGE</b> 1 of 7 |
| <b>PROCEDURE TITLE:</b>     | Guidelines for Use of Miami Dade College Computing Resources |                    |
| <b>STATUTORY REFERENCE:</b> | FLORIDA STATUTE 1001.64                                      |                    |
| <b>BASED ON POLICY:</b>     | VII-1 Use of Computing Resources at Miami Dade College       |                    |
| <b>EFFECTIVE DATE:</b>      | September 10, 2002   |                    |
| <b>LAST REVISION DATE:</b>  | November 8, 2005   |                    |
| <b>LAST REVIEW DATE:</b>    | November 8, 2005   |                    |

## **PURPOSE**

To provide guidelines for College students, faculty, staff, retirees, alumni and guests who have been authorized to use (collectively, this group shall be referred to as “Users”) components of Miami Dade College’s “Computing Resources” (defined below).

A Computing Resources User at the College includes any User who accesses any of the College’s Computing Resources from any location (physical, logical, on-site and remote). This definition also includes any person who accesses the College’s Computing Resources via an electronic network, or who uses the College’s Computing Resources to connect a personal computer to any other system or service including one that is individually owned.

### **I. Definition of Terms**

Unless otherwise stated, the terms used in this procedure are consistent with those defined in Chapter 815.03 of the Florida Computer Crimes Act.

Computing Resources at Miami Dade College include, but are not limited to, mainframe computer systems; personal computers; minicomputers; file servers; printers; workstations; local area networks (LANs) (A geographically limited communication network that connects users within a defined area); the wide area network (WAN) (A communications network that connects computing devices over geographically dispersed locations); Internet access terminals; disks, tapes and other storage media; software; software applications; electronic mail, including attachments to electronic mail messages; voice communications infrastructure; voice mail, instructional laboratories; and, with regard to the aforementioned, all associated tools, instruments, and facilities.

Electronic Communication at the College is any data, email, voice mail, or information sent or retrieved utilizing any Computing Resources owned, operated or supported by the College.

Intellectual Property at the College means any and all Copyrightable Works, Inventions, Tangible Research Materials, Trademarks or Trade Names and Trade Secrets (which are described in detail in Policy I-10, Article 11 of the UFMDCC Faculty Contract).

## II. Computing Resources Information

The College owns all Computing Resources, including any data or information stored on the College's Computing Resources, except for information covered by licenses and other intellectual property rights. Individuals authorized by the College may monitor all Computing Resources to ensure appropriate use subject to applicable Laws (defined below).

## III. Legal Responsibilities

### A. Lawful Use

All uses of the College's Computing Resources shall be subject to federal, state and local laws, College policies and procedures, and the rules of various departments, areas, laboratory and others, as appropriate (collectively the 'Laws'). All Users should consult the Florida Computer Crimes Act, Florida Statutes Chapter 815; The U.S. Patriot Act of 2001; the Miami Dade College catalog, the Student Rights and Responsibilities Manual, and the College policies and procedures as appropriate. These Laws, policies and procedures, and rules may be found in Campus libraries or on the Internet.

### B. Intellectual Property Rights of College and Others

Users must respect all Intellectual Property rights of the College as defined in applicable College Policies and Procedures, the UFMDCC Faculty Contract (Article 11), and all Intellectual Property rights of others, when accessing information through the College's Computing Resources.

### C. Contracts

All use of the College's Computing Resources must be consistent with all College contractual obligations, including limitations defined in software and other licensing agreements.

## IV. Security

### A. Concealed Identity

Users must not conceal their identity when using the College's Computing Resources, except when anonymous access is explicitly provided. Altering electronic communications to hide one's identity or to impersonate someone else is prohibited and in violation of applicable Laws.

## B. Unauthorized Access

Users must not make, or attempt to make, any deliberate unauthorized use of or changes in official data on the College's Computing Resources. Examples of unauthorized use of the College's Computing Resources include but are not limited to the following:

1. Unauthorized reading of electronic communications of other Users.
2. Accessing confidential College files without authorization.
3. Using or divulging protected information that was read by mistake or other cause.
4. Use of another individual's user ID or password (obtaining, possessing, using or attempting to use someone else's password; sharing with or allowing another individual to use your user ID or password).
5. Unauthorized copying of software or other media licensed only to the College to Users' personally owned equipment.
6. Unauthorized copying of software or other media licensed by any other individual or entity to College equipment.
7. Theft or destruction of computer software or hardware.
8. Theft or destruction of documents files or programs created through use of College equipment or software.
9. Use of College equipment, software, or data to perpetrate fraud.
10. Use of College equipment to libel, slander, threaten, intimidate, or harass any other person, or to otherwise violate any law or College policy.
11. Using any computer as a server without authorization from the College.
12. Any commercial advertising or commercial purpose not expressly authorized by the College.
13. Solicitation of contributions for political, charitable or other causes not authorized by the College or applicable Laws.
14. Any business activities not authorized or sponsored by the College.
15. Sending chain letters, scams and pyramid schemes, bomb threats and hoaxes, spamming (distributing unsolicited email or advertisement to Users), or denial of service attacks (see IV-E below).
16. Attempting to defeat any security on any computer or system or to spread any

computer virus.

17. Unauthorized and illegal tapping of phone lines or network transmissions, including wireless transmission (e.g. using network sniffers).
18. Releasing a virus, worm, or other programs that may damage or harm the network.
19. Any criminal activity.
20. Any conduct that violates applicable Laws.
21. Any unethical or immoral conduct, such as using the College's Computing Resources to access child pornography or distribution of pornography to minors.
22. Unauthorized reproduction or use of any College, names, trademarks and/or logos.

#### C. Security Compromise

Users must not defeat or attempt to defeat any Computing Resources security systems, such as "cracking" or guessing user identifications or passwords, compromising room locks or alarm systems.

Users must not attempt to scan College Computing Resources from an internal or external network for the purpose of discovering vulnerabilities, except for authorized MDCC Network and Telecommunication staff and other authorized individuals. In cases of security compromises, authorized Network and Telecommunication staff is authorized to disconnect and/or disable access to protect the integrity of the College Network.

#### D. Data Interception

Users must not intercept or attempt to intercept data communications not intended for their use or access.

#### E. Denial of Service

Users must not deny, interfere with, or attempt to deny or interfere with service to other Users through the use of such means as resource domination or distribution of computer worms, viruses, etc.

#### F. Personal Responsibility

Users are responsible for the privacy and security of their Computing Resources such as User IDs and passwords. Any User change of password must follow published guidelines (College Procedure 7932). IDs and passwords are assigned to each individual User and are not to be shared with any other person. Users are personally responsible for all transactions conducted under their personal user ID and/or password. Users shall report any attempted

security violations to the proper college authority.

## V. General Responsibilities

### A. Proper Authorization

Users must have prior authorization to use any College Computing Resources. Users must not permit or assist any unauthorized person to access College Computing Resources.

At least once a year, all College-related Users will be required to acknowledge their compliance with College Computing Resources policies and procedures. Failure to comply will prevent the Users from accessing the College's Computing Resources.

### B. Downloading Information Using the College's Computing Resources

Unless authorized by state and federal law, including the TEACH Act, users of the College's Computing Resources who download any software, files, materials or information of any type using the College's Computing Resources:

- Must comply with all terms of any software license agreements, end user license agreements, terms of use, privacy policies and any other agreements or policy that a User has notice of (collectively "License Agreements").
- Must be aware that copyright protection includes, but is not limited to, computer software, recordings of songs, graphic art, photographs; using material that is protected by copyright is illegal, unless the User has received express permission from the owner of the copyright, such as if the material is explicitly labeled as being in the Public Domain.
- Must not copy or download any materials protected by copyright, such as software, songs, image files or other similar materials, for any purpose outside those allowed by the License Agreement that pertains to such software, songs or image files.
- Must not make software, songs, image files or other similar materials available for others to use or copy in violation of the License Agreement.
- Must not accept unlicensed software, songs, image files or other similar materials from any third party.
- Must not install or direct others to install illegal copies of software, songs, image files or other similar materials onto any College-owned or operated Computing Resource.

### C. External Data Networks

Users must observe all applicable policies of external data networks. It is the responsibility of the User to read and understand the data security rules published by any external data network accessed by a College User. Any violation of the data security regulations of an external network is considered by the College to be a violation of its own regulations, policies or procedures.

### D. Personal Identification

Users accessing College Computing Resources must show identification upon request.

E. Access to Data

Users must allow authorized College personnel access to data files kept on College Computing Resources for the purpose of systems backups, investigation of problems or for any other necessary purpose. Users must also provide access to their supervisor or other College personnel as directed by their supervisor, department manager or other College official in authority.

F. Internet Access

User access to the Internet and Internet services is a privilege not a right. Access entails personal responsibility and all Users must comply with all applicable Laws.

G. For-profit Use

Without specific authorization, all activities using College Computing Resources for profit are prohibited. However, this is not meant to restrict normal communications and exchange of electronic data, consistent with the College mission and its policies and procedures.

H. Inappropriate Electronic Communications

Knowing or reckless distribution of unwanted mail or other electronic communication is prohibited. Specifically, denial of services, broadcast, chain letters, ping bombs, and other unauthorized schemes that may cause excessive network traffic or computing load is absolutely prohibited. Further, College Computing Resources shall not be used to endorse, promote, lobby, or raise money for any political candidate or political organization. In addition, College Computing Resources shall not be used to solicit charitable contributions, except for solicitations authorized by the College and subject to applicable Laws.

I. Installation or Modification of Data or Equipment

Without specific written authorization, use of College Computing Resources must not cause, permit, or attempt any installation of hardware or software, destruction or modification of data or equipment.

J. Removal of Equipment or Documents

Users must not destroy or remove any College Computing Resources, including, but not limited to College-owned or administered equipment, data or documents without specific prior written authorization of the College.

## VI. Violations

### A. Reports of Violations

Users must report any violations of this Procedure to the appropriate Campus President, Vice Provost, appropriate Dean, or area head. Users must not conceal or help to conceal violations by any party. Any such concealment or attempted concealment of violations committed by another party shall constitute a violation of these rules to the same extent as the actual violation.


### B. Penalties For Violations

The College is authorized to apply certain penalties to enforce its policies and regulations and to preserve the integrity of the College's Computer Resources including data, facilities, and/or User services. (Refer to the College policies and procedures governing the behavior of employees, the UFMDCC Faculty Contract, and the Students' Rights and Responsibilities Handbook informing students of College policies and procedures governing student conduct). Penalties may include, but are not limited to suspension with or without pay, termination of employment, student suspension or dismissal, temporary or permanent reduction or elimination of access privileges that may apply to Computing Resources, networks, rooms, programs, other technological resources services or facilities. The User shall be notified of any action taken by the College.

If a violation or suspected violation may warrant action beyond a College imposed penalty, or may create a liability for the College, the case may be referred to the proper legal authority.

## VIII. Due Process

College employees shall have at their disposal the right to exercise those due process rights and procedures which are outlined in College policy and procedures and the UFMDCC Faculty Contract governing the terms and conditions of employment. Students shall have at their disposal the right and privileges determined by the Student Rights and Responsibilities Handbook.

|  |             |
|--|-------------|
|  |             |
| 11/8/05  |             |
| <b>PRESIDENT</b>   | <b>DATE</b> |