**SUNY Downstate Health Sciences University**
**Computer Standards & Policies**

The following computer policies and standards have been established centerwide for Downstate Medical Center:

1. Policy DCC04A: Desktop Standards and Policies

2. Policy DCC04B: Network Cabling Procedures

3. Policy DCC04C: Unix Security Policies

4. Policy DCC04D: Wireless Network Policies

5. Computer and Network Usage Policy

Note: these policies have been developed in conjunction with, and reviewed by, the Downstate Departmental Computer Coordinators Group.

**POLICY DCC04A** June 10, 2004

# Desktop Standards and Policies

For Downstate Medical Center

| | | |
|---|---|---|
| HARDWARE: | File servers: | Compaq/HP |
| | Desktops: | Dell, Mac |
| | Network: | Cisco |
| SOFTWARE: | Operating Systems: | NT, WIN 2000, XP<br>MAC OS 9 & 10 |
| | Word Processing: | Word |
| | SpreadSheet: | Excel |
| | DataBase: | Access |
| | Presentation: | PowerPoint |
| | Course Dev/Mngmnt: | WebCT, SLN, Prime |
| | Scheduling: | Lotus Notes |
| | Internet Browser | Internet Explore 5.5+, Netscape 4+ |
| | Anti-Virus | Norton: Corporate Edition |
| | E-mail: | Lotus Notes |

Notes:

1. These standards are generic to Downstate PCs and MACs; specific departments or applications may be more restrictive.
2. Norton Anti-Virus Corporate Edition must be installed on all PC, MAC, and laptop devices connected to the Downstate network, and must be regularly checked to insure that the Virus Definition File is current; otherwise the device may be disconnected from the network. To verify that your device PC has current anti-virus software (Norton Corporate Edition) that is fully operational: Double click yellow shield icon (found at right bottom of the desktop screen) and verify that you have a current Virus Definition File; Otherwise, please go to the following web site http://uhweb1.hscbklyn.edu/netgrp/
3. All PC users must regularly check and verify that their operating systems (OS) and systems software are up-to-date with all important security updates, patches, and service packs; otherwise the device may be disconnected from the network. To check: go to the following web location http://windowsupdate.microsoft.com/ and click Scan for Updates (Product Updates for Windows NT) and follow the instructions.
4. Minihubs (whereby a single network port is sub-divided into multiple connections) are not permitted on the Downstate network.
5. Individual departments may choose to utilize other office automation software; however there will be no centerwide support for these software modules.
6. Wireless Networks: Security concerns require that all wireless networks at Downstate must be coordinated through and approved by NTG (see policy no. DCC04D below)
7. Naming convention for all PCs and MAC computer/machine names: must include current location (for example : BIOCHM-BSB-7-5B)

**PROCEDURE DCC04B** January 29, 2003

# Network Cabling Procedures

## Objective:

To provide for our entire Downstate community a computer network environment that is highly reliable and highly available our computer network has been designed to provide full functionality, appropriate bandwidth, high degree of security, and capacity for growth in a cost-effective manner. Our campus network technology group uses high-quality, standardized equipment, installed & maintained by well-trained personnel, with appropriate environmental controls, and in compliance with all facilities/building code requirements

## Procedures:

The responsibility for the Downstate computer network lies with the campus network technology group (NTG). To insure a continuing highly degree of reliability, availability, and security, the following activities must be coordinated through and approved by NTG staff for ALL computer cabling at Downstate Medical Center:

1. Initial purchase requisition
2. Vendor selection
3. Management of network installation
4. Review and payment approval upon completion of installation (with FMD approval)
5. Any changes or additions to the network configuration in any data closet.
6. Access to all data closets is restricted to authorized / NTG staff.
7. Patching of a new line should only be done when PC/device install is imminent.

To request network cabling, of if questions arise, please contact Robert Williams by e-mail or at x4593, or our new helpdesk at 270-HELP or email to Technical Support

Wireless Networks: Security concerns require that all wireless networks at Downstate must be coordinated through, and approved by, NTG.

**POLICY DCC04C** January 29, 2003

# UNIX SECURITY GUIDELINES

Here are a number of security directives addressed to Unix SA's:

1) If you have not configured ipchains, ipfilters, or iptables, ensure that you are using TCP wrapers. This is very simple to set up, and works with all Unix varieties.

2) Ensure that direct root access is only possible on the console. This means that outside intruders have to get both a user and a root password to get in directly.

3) Eliminate all .rhosts and hosts.equiv files.

4) If you are using NFS to export file systems, ensure that only the machines that you want can mount the file systems.

**POLICY No. DCC04D** Oct. 03, 2003

## Wireless Network Policies

To see the detailed Wireless Network Policies (No. DCC04D) at Downstate, please contact the Network Technology Group (NTG) at 270-2593 or send email requesting a copy of this policy to Technical Support.

As a general rule, all wireless networks at Downstate must be coordinated through and approved by NTG; any unauthorized wireless access point will be disconnected from the Downstate network.

July, 1997

# STATE UNIVERSITY OF NEW YORK AT BROOKLYN
# DOWNSTATE MEDICAL CENTER
# COMPUTER and NETWORK USAGE POLICY

## I. INTRODUCTION

Access to modern information technology is essential to the state university mission of providing the students, faculty, clinicians and staff of the State University of New York Downstate Medical Center (SDMC) with educational, clinical, and research services of the highest quality. The pursuit and achievement of the SDMC mission of education, research, clinical service, and public service require that the privilege of the use of computing systems and software, internal and external data networks, as well as access to the World Wide Web, be made available to all those of the SDMC community. The preservation of that privilege for the full community requires that each faculty member, clinician, staff member, student, and other authorized user comply with institutional and external standards for appropriate use.

To assist and ensure such compliance, SDMC establishes the following policy which supplements all applicable SUNY policies, including sexual harassment, patent and copyright, and student and employee disciplinary policies, as well as applicable federal and state laws.

## II. GENERAL PRINCIPLES

1. Authorized use of SDMC-owned or operated computing and network resources shall be consistent with the education, research, clinical, and public service mission of the State University of New York, and consistent with this policy.

2. Authorized users of SDMC computing and network resources include faculty, staff, students, and other affiliated individuals or organizations authorized by SDMC. Use by non-affiliated institutions and organizations shall be in accordance with SUNY Administrative Procedures Manual Policy 007.1: Use of Computer Equipment or Services by Non-affiliated Institutions and Organizations.

3. This policy applies to all SDMC computing and network resources, including host computer systems, SDMC-sponsored computers and workstations, software, data sets, and communications networks controlled, administered, or accessed directly or indirectly by SDMC computer resources or services, employees, or students.

4. The SDMC reserves the right to limit access to its networks when applicable campus or university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor or generally restrict the content of material transported across those networks, unless required for security or network performance reasons.

5. The SDMC reserves the right to remove or limit access to material posted on university-owned computers when applicable campus or university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor the content of material posted on university-owned computers.

6. The SDMC does not monitor or generally restrict material residing on SDMC computers housed within a private domain or on non-SDMC computers, whether or not such computers are attached to campus networks.

7. The SDMC reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including individual login sessions to determine if a user is violating this policy or state or federal laws.

8. This policy may be supplemented with additional guidelines by campus units which operate their own computers or networks, provided such guidelines are consistent with this policy.

## III. USER RESPONSIBILITIES

**Privacy:** No user should view, copy, alter or destroy another's personal electronic files without permission (unless authorized or required to do so by law or regulation).

**Copyright:** Written permission from the copyright holder is required to duplicate any copyrighted material. This includes duplication of audio tapes, videotapes, photographs, illustrations, computer software, and all other information for educational use or any other purpose. Most software that resides on SDMC computing network (s) is owned by the University, SDMC, or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on SDMC computing network (s) or for distribution outside the University; against the resale of data or programs, or the use of them for non-educational purposes or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization.

**Harassment, Libel and Slander:** No user may, under any circumstances, use SDMC computers or networks to libel, slander, or harass any other person.

**Access to Computing Resources:**

**- Accounts:** Accounts created by a system administrator for an individual are for the personal use of that individual only.

**- Sharing of access:** Computer accounts, passwords, and other types of authorization are assigned to individual users and should not be shared with others. You are responsible for any use of your account. If an account is shared or the password divulged, the holder

of the account will lose all account privileges and be held personally responsible for any actions that arise from the misuse of the account.

**- Permitting unauthorized access:** You may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.

**- Termination of access:** When you cease being a member of the campus community (e.g., withdraw, graduate, or terminate employment, or otherwise leave the university), or if you are assigned a new position and/or responsibilities within the State University system, your access authorization must be reviewed. You must not use facilities, accounts, access codes, privileges or information for which you are not authorized in your new circumstances.

**Circumventing Security:** Users are prohibited from attempting to circumvent or subvert any system's security measures. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

**Breaching Security:** Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any SDMC computer or network is prohibited. Breach of security includes, but is not limited to, the following:

- Creating or propagating viruses.
- Hacking.
- Password grabbing.
- Disk scavenging.

**Abuse of Computer Resources:** Abuse of SDMC computer resources is prohibited and includes, but is not limited to:

- **Game Playing:** Limited recreational game playing, which is not part of authorized and assigned research or instructional activity, is acceptable, but computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility must give up the use of the terminal when others who need to use the facility for academic or research purposes are waiting.

- **Chain Letters:** The propagation of chain letters is considered an unacceptable practice by SUNY and is prohibited.

- **Unauthorized Servers:** The establishment of a background process that services incoming requests from anonymous users for purposes of gaming, chatting or browsing the Web is prohibited.

- **Unauthorized Monitoring:** A user may not use computing resources for unauthorized monitoring of electronic communications.

- **Flooding:** Posting a message to multiple list servers or news groups with the intention of reaching as many users as possible is prohibited.

- **Private Commercial Purposes:** The computing resources of SDMC computers and networks shall be in accordance with University policy on use of University facilities for political purposes (SUNY Administrative Procedures Manual Policy 008, Attach. A).

## IV. LIMITATIONS ON USER'S RIGHTS

1. The issuance of a password or other means of access is to assure appropriate confidentiality of SDMC files and information and does not guarantee privacy for personal or improper use of university equipment or facilities.

2. SDMC provides reasonable security against intrusion and damage to files stores on the central facilities. SDMC also provides some facilities for archiving and retrieving files specified by users, and for recovering files after accidental loss of data. However, the SDMC is not responsible for unauthorized access by other users or for loss due to power failure, fire, floods, etc. SDMC makes no warranties with respect to Internet services, e.g., Netscape, and it specifically assumes no responsibilities for the content of any advice or information received by a user through the use of (campus') computer network.

3. Users should be aware that SDMC computer systems and networks may be subject to unauthorized access or tampering. In addition, computer records, including e-mail, are considered "records" which may be accessible to the public under the provisions of the New York State Freedom of Information Law.

## V. WEB POLICY

The SDMC World Wide Web Home Page is an official publication of the SDMC. Unless otherwise indicated, all materials, including text and photographs, appearing on the Home Page or subsequent official home pages of specific departments are copyrighted and should not be reproduced without written permission from (campus officer). Home pages lined to SDMC Home Page maybe created by academic departments, programs, centers or institutes, administrative departments, or recognized student groups. Individual members of the faculty and staff may create their own, but must line them through their department's home page.

Individual students may create their own home page. Each student home page shall include the disclaimer that neither the page contents nor the link identifiers are monitored, reviewed, or endorsed by SDMC.

## VI. SANCTIONS

Violators of this policy will be subject to the existing student, faculty, or employee disciplinary procedures of SDMC. Sanctions may include the loss of computing privileges. Illegal acts involving SDMC computing resources may also subject users to prosecution by State and federal authorities.

---

Note: This policy was drafted and disseminated to all SUNY campuses by SUNY-Central in November 1996, and reviewed and accepted by the Downstate Academic Computing Committee in July 1997. This policy is currently under review.