



**Metropolitan State College of Denver
Information Technology Policies and Guidelines**

Approved By: President's Cabinet

Table of Contents

- I. Introduction: Academic Freedom & Confidentiality
- II. Responsible Use of Information Technology Resources
- III. Copying Computer Software
- IV. Microsoft Suite Users Acceptance
- V. Electronic Mail Policy & Procedures
- VI. Use of Intel® LanDesk® Management Suite
- VII. Computer Technology Procurement Policy
- VIII. Use of Contract Personnel
- IX. Guidelines for Electronic Mailing Lists by Major
- X. Use of Napster and Similar Software Programs
- XI. Web and Internet Technology Policy
- XII. Kiosk Idle Loop Usage
- XIII. Electronic Communication Policy (Administrative Policy #34)
- XIV. Broadcast Messages (Voice and E-mail) (Administrative Policy #35)
- XV. Ad Hoc Access to Banner Databases Policy
- XVI. BANNER Security Policy
- XVII. Use of Wireless Networking Devices at Metropolitan State College of Denver
- XVIII. IT Governance Policy
- XIX. Network Security Policy for Metropolitan State College of Denver
- XX. Electronic Survey Policy and Guidelines for Metropolitan State College of Denver
- XXI. Password Policy for Metropolitan State College of Denver
- XXII. Automatic Timeout of Idle Sessions

The Division of Information Technology is committed to providing the highest quality and most responsive service possible to the MSCD community with the resources available. The policies and guidelines that follow are intended to ensure that level of service. However, IT recognizes that departments, faculty and staff have special technology needs, which must be addressed so that they can provide students the optimal educational experience or service. For those policies or guidelines that do not specifically outline a process for accommodating a special need, requests should be submitted to the appropriate Dean or Vice President who will discuss the issue with the Vice President for Information Technology for his or her consideration.

I. Introduction: Academic Freedom, Confidentiality and Privacy

Metropolitan State College of Denver endorses the principle of Academic Freedom, understood to mean freedom to discuss academic subjects fully, freedom to engage in research and to publish the results of research, and freedom to write or speak as citizens without fear of institutional censorship or discipline, provided individuals do not represent themselves as speaking for the College. Policies concerning Information Technology (IT) will be administered with full respect for the principle of Academic Freedom.¹

Further, the College understands the importance of securing the confidentiality of research data and other academic materials. In a networked electronic environment it is not within the means of the College to provide absolute assurances of confidentiality with respect to data stored on College equipment. However, the College offers employees training in how to protect against disclosure of electronically recorded information. Faculty members, particularly, are encouraged to seek training and advice from IT that will empower them to protect confidential information related to their academic work.

The Colorado Open Records Law designates most electronic documents created by state employees as public records accessible upon request. Major exceptions include student records (which are protected by federal law), personnel files, and research data. Only employees of the College who need access to confidential records to do their work can access these files. These employees are under a legal obligation not to disclose or use them for any other purpose.

A fuller discussion of Academic Freedom, confidentiality and privacy can be found in the new "Responsible Use Policy" and the e-mail Policy found in the IT Policies and Guidelines.

1. Trustee's Handbook for Professional Personnel, Section III.

II. Responsible Use of Information Technology Resources

I. Purpose:

Information Technology at MSCD is an educational and administrative resource for all faculty, staff and students. IT serves as a major means of official communication with the public, and is also a business asset. At the same time, the sense of community at MSCD consists of personal as well as professional relationships. MSCD is a place where freedom of expression and inquiry is valued and protected. It is important to establish a balanced approach to the use of IT resources-one that facilitates all these priorities.

Respect for the views of others with whom we disagree is important if we are to get the full benefit of our expressive freedom, and demonstrating mature judgment is an important element of personal integrity and credibility. Therefore, MSCD encourages IT users to follow the Ten Principles of Civility in Cyberspace. However, although rude or impolite behavior such as "flame wars", "hate speech", spammed solicitations, and off-topic-list postings may be annoying, occasional breaches of civility do not violate specific laws or rules.

II. Policy:

The same rules and laws that apply in physical space also apply in cyberspace. Standards of academic freedom and professional conduct for employees, and the rights and responsibilities of students govern conduct online as much as they do in the hallways, offices and classrooms. Unauthorized access to and sharing of confidential student information (including computer passwords), or certain electronic confidential employment records (including computer passwords) violates state and federal law. Illegal activity such as copyright infringement, patent infringement, fraud, forgery, distribution of child pornography and forms of criminal harassment, including bomb threats and hoaxes is just as criminal online as elsewhere. Moreover, some special laws apply to the electronic environment, including State and federal computer security laws and laws prohibiting interference with college operations. Downloading material that violates the College's legal obligations and contractual commitments (e.g. software and recording piracy) will not be tolerated. Finally, actions that adversely affect MSCD IT resources, or the ability of others to use them are prohibited. For example, e-mail, bombing, spamming, and releasing or operating a damaging program such as a virus, could result in cessation of the offender's access to IT resources in addition to other penalties, such as College Disciplinary action, up to and including termination of employment or expulsion from the College.

Within the above restrictions, employees and students may use MSCD's IT resources for incidental, non-commercial personal communication so long as such use clearly and specifically communicates to the viewer that the individual is speaking in a personal capacity and not for the College. However, users should be aware that, although MSCD will not routinely monitor communications or

search individual computer files, individual privacy cannot be guaranteed with respect to personal communication and related records. Most computer data and documents created, used, or maintained by MSCD employees are not confidential: and must be disclosed to the public on request under the Colorado Open Records Act. In addition, MSCD cannot prevent individuals from monitoring unencrypted e-mail sent through outside servers.

MSCD IT staff members are authorized and able electronically to access electronic programs, data, and files stored on College equipment as may be necessary to perform their duties. Except in emergencies, they will notify users and specify a time before accessing desktop computers and files. Any objections to IT staff access should be addressed in writing to the department chair or director-level supervisor and to an IT administrator at the director level. IT staff in the course of their duties may find evidence of illegal or unauthorized activity. If they do, their responsibility is to report such evidence in writing to their director. Authorization may be granted for a full search of computer programs and data. In that event, the user will be notified.

Revised: December 2004

Approved December 2001

III. Copying Computer Software

I. Purpose:

Respect for intellectual effort and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in media.

Because computer software is easily reproduced, respect for the work and creativity of others is especially critical. The College has both a legal and ethical responsibility to prevent unauthorized duplication and distribution of software.

Since unauthorized copying of software by individuals can harm the entire College, subjecting it to legal liabilities and making it more difficult to negotiate agreements that make software available at reasonable cost, it is the purpose of this policy to clarify the ramifications of such duplication and distribution, and to prevent such action.

Responsibility

It is the responsibility of all users of computer software to read and be aware of the terms and conditions of an acquired software product's license agreement, and to abide by such agreement. It is the responsibility of professionals and skilled workers who provide information services and products, including instruction in the use of software resources, to refrain from copying and distributing software and related documentation, except as specifically authorized by licensed agreement, but also to clearly inform clients they are responsible licensees of such proprietary products.

II. Policy:

Metropolitan State College of Denver acquires software licenses, and must use the software and documentation only in accordance with applicable license agreements. The College does not own such software or its related documentation. Except as specifically authorized by a software licensor in an agreement, College employees and students are prohibited from reproducing licensed software or related documentation.

It is the responsibility of software users to be aware of limitations on use and reproduction described in the license agreement related to specific software and to use licensed software strictly in accordance with such limitations. A copy of the software license agreement should be kept with the software for easy reference to determine if copies can be made, e.g., for backup or archival purposes, and to assure compliance with all provisions of the software agreement. If a department purchases software outside of the standard for MSCD, it is responsible for licensing, compliance, maintenance and service for the software.

College employees or students making, acquiring or using unauthorized copies of licensed software or related documentation, or otherwise misusing licensed

software may be disciplined by the College as appropriate. The individual may also be subject to civil damages of \$100,000 or more, and criminal penalties including fines and imprisonment.

Recommended penalties for violation(s) of software copyright licenses are as follows:

For students: The MSCD Student Handbook delineates appropriate penalties for violations of college policies, up to and including suspension and expulsion from the College.

For administrators, faculty and staff (including student employees): Penalties range from a verbal reprimand through dismissal, depending upon the circumstances of the violation(s) of software copyright.

Applicability, Definitions and Reference

Applicability:

This policy applies to all officers, faculty, staff, students, Schools (LAS, SPS, and Business) and operations of Metropolitan State College of Denver.

Definitions:

Software: A computer program or set of programs held in some kind of storage medium and loaded into read/write or random access memory (RAM) for execution.

Reference:

U.S. Copyright Law ².

"Using Software. A Guide to the Ethical and Legal Use of Software for Members of the Academic Community."³ produced by Educause, a non-profit consortium of over 450 colleges and universities committed to the use and management of Information Technology in higher education, and ADAPSO, the computer software and services industry association

² See <http://www.loc.gov/copyright/title17> for complete text of US Copyright Law.

³ For text from Educause member college, see <http://wjh-www.harvard.edu/wjh/computing/educom.html>.

Frequently Asked Questions about Software Copying⁴

What is software piracy, exactly?

It is the unauthorized duplication, distribution or use of computer software -- for example, making more copies of software than the license allows, or installing software licensed for one computer onto multiple computers or a server.

Copying software is an act of copyright infringement, and is subject to civil and criminal penalties. It is illegal whether one uses pirated software oneself, gives it away, or sells it. And aiding piracy by providing unauthorized access to software or serial numbers to registered software is illegal.

What's the harm in making a few extra copies?

If those extra copies are used on College-owned computers, the harm could be great. Software publishers take piracy very seriously. The College and the individuals involved could be held liable for large monetary damages.

In the larger picture, copying is unethical and cheats the publisher and everyone who uses the software. It makes software more costly and denies the publisher the sales it needs to improve software and finance new projects.

How will MSCD ever find out that I have illegal software?

It happens more often than you might think, from honest employees and students, routine software audits, technology support professionals, network administrators, software publishers and piracy watchdog groups.

Your work computer is College property. So is your connection to the Internet via the campus network. MSCD is committed to making sure that its computers run legally licensed software, and that its network is not supporting software piracy in any form.

What happens when illegal software is found?

If illegal software is reported to a software publisher or piracy watchdog group, legal action can be brought against MSCD and the individuals involved. At minimum, the College will have to prove that it has resolved the problem, which typically requires an intensive software audit within a very short timeframe. Other sanctions can include large monetary damages, or exclusion from discount pricing and volume-licensing programs, such as the Microsoft Office license agreement.

⁴ Metropolitan State College of Denver acknowledges the work of [Cornell University](#) in the development of these questions and answers.

Our software budget wasn't big enough this year. Can we make copies for now and buy enough for everyone next year?

No. Unless otherwise stated in the software license, the only copy you can legally make is one archival backup of the original installation disks or CD, to be used only if the originals fail.

When my computer was delivered, it had software installed on it. Is this software already legally licensed?

Yes, if it was obtained through the Division of Information Technology. If your computer came from another source, review the licenses and documentation to verify the software's legitimacy.

I require my students to use certain software for assignments. Since I'm using it for educational purposes, I can give them copies, right?

No. And there's little chance that the "fair use"⁵ argument can be applied to software the way it can to printed materials - it's generally impossible to install and use only a small piece of a software product.

I'm trying to decide which software package to buy. Can I install my co-workers' software just to try it, if I remove it right after I'm done?

No. There's a widespread myth that you can use software for 24 hours without penalty. The truth is the software is illegal the moment you install it. Arrange to use your co-workers' computers instead. Or ask the software publisher for a trial version.

If MSCD has a site license for something, does that mean we can copy it to as many computers as we want?

Not necessarily. Each site license states who may use the software, where and for what purpose. Within those restrictions, a site license allows unlimited use. Most of MSCD's site licenses permit MSCD to install the software on their College computers; a few include home computers and student-owned computers as well.

⁵ See United States Code Title 17§1: Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phono-records or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include -(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

Can I put MSCD site-licensed software on a computer MSCD doesn't own -- for example, my home computer?

Usually not, as most of MSCD's site licenses are restricted to College or student owned computers, unless otherwise directed, i.e.: The Microsoft Campus Agreement.⁶

I work at home sometimes. Can I copy software from my work computer to my laptop or home computer, since I won't be using both at the same time?

Some software publishers allow this type of use; others do not. Read the license agreement to determine what type you have.

A friend recommended some great software, but the publisher is out of business. Would it be OK to get a copy from my friend?

Your best bet is to ask the copyright holder for written permission to copy the software.

Where can I obtain the licenses?

Licenses can be picked up at the Division of Information Technology Help Desk on the 4th floor of the Administration Building.

I still have some questions. Who can I ask?

Call the Division of Information Technology at (303) 556-8325 or send an e-mail to: helpdesk@mscd.edu

⁶ Microsoft Campus Agreement

Metropolitan State College of Denver (MSCD) has entered a Campus Agreement with the Microsoft Corporation effective 09/01/01 through 08/31/02. This agreement allows "faculty and staff (with the exception of student workers) the right to run one copy of the Software, for school-related activities, on either a laptop or desktop that they own or lease." In addition MSCD's faculty and staff can use the entire platform of software for schoolwork at home. During the Campus Agreement term, a Special Product Key will be generated for the licensed staff and faculty members at MSCD. The Special Product Key is assigned to each staff and faculty member and is intended for the sole use of the user who is granted the Special Product Key. Holders of these key codes are required to keep their Special Product Keys secure, by not sharing them with unauthorized users.

Excerpt from the agreement:

"The Campus Agreement program gives your Users the right during this agreement to run a platform of 'Software' (Microsoft Windows or Windows NT, Workstation Upgrades; Microsoft Office Standard or Office Professional; Microsoft FrontPage; Microsoft Visual Studio Professional Edition; Microsoft BackOffice Client Access License; and MS Press Office Starts Here Step-by-Step Interactive and add-on products."

The Campus Agreement software is available for pickup at AD475, each employee must show MSCD ID. Please contact the Help Desk at 303-556-8325 for more information.

IV. Microsoft Suite Users Acceptance Form

The Microsoft Suite of software is made available to employees of Metropolitan State College of Denver (MSCD) because the college purchased a Microsoft Campus Agreement. The Agreement is renewed annually. MSCD is extending to employees the right to use this software for **school-related** purposes at home. Employees do not own the license or the CDs, but are leasing the license and CDs from MSCD for the term of the agreement. Employees will be required to remove the software from their home machine if the Campus Agreement is not renewed by MSCD or upon leaving the employment of the college. **Employees are not licensed to use the Software at home for personal purposes.**

MSCD received a Special Product Key that allows multiple installations of Microsoft Office product. This Special Product Key will be distributed to staff/faculty users as needed. Holders of this Special Product Key are required to keep it secure and only distribute it to employees authorized to install and distribute the software on the designated machines. You will be held responsible for unauthorized use of your unique Special Product Key.

The Microsoft Campus Agreement grants MSCD the right to use copies of the following software:

Any version of Microsoft Windows or Windows NT Workstation Upgrade
Microsoft Office Standard or Office Professional
Microsoft FrontPage
Microsoft Visual Studio Professional Edition
Microsoft BackOffice Client Access License
MS Press Office Starts Here Step-by-Step Interactive

V. Electronic Mail Policy and Procedures Principles, Policies, User Responsibilities, and Information Technology (IT)

I. Purpose:

Proper usage. Electronic Mail (e-mail) is provided as a professional resource to assist MSCD students, faculty and staff in fulfilling the educational, research, communication and service goals of MSCD. Incidental personal use is permitted as long as it does not have negative effects on any other e-mail account, jeopardize the e-mail system, interfere with your job or violate the law or any other provision of the MSCD Appropriate Use Policy or of any other policy or guideline of Metropolitan State College of Denver. Each user is responsible for using the e-mail system in a professional, ethical, and lawful manner. Material that is fraudulent, harassing, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate; may not be sent by e-mail or by other forms of electronic communications. MSCD reserves the right to revoke e-mail and related privileges from any individual violating these policies.

II. Policy:

(1) **Responsibilities.** The use of each account is the personal responsibility of the account holder. The contents of e-mail will not be monitored, censored, or otherwise examined except with specific authorization and direction by the College Attorney or as part of the required system administration as described below.

(2) **Disguising and or impersonating e-mail identities; "spoofing."** Users should not disguise their identity or user name while using the MSCD e-mail system or alter the 'From:' line or any other indications of origin on e-mail or postings. Behavior of this type violates the guidelines for student and professional conduct and is equivalent to fabricating identities on any other written document.

(3) **Chain e-mail.** Users should not initiate or forward chain e-mail. Chain e-mail is a message sent to a number of people asking each recipient to send copies with the same request to others.

(4) **Sending unsolicited e-mail; "spamming."** Users should not send unsolicited, non-school related e-mail to persons with whom they do not have a prior relationship.

(5) **Virus prevention:** The e-mail server examines all messages flowing through it and will reject those that it determines to contain a virus. When this happens, a reply is sent to the message origin stating why the message was rejected. The ability of the e-mail server to ascertain virus content is not guaranteed. Additionally, if e-mail is being read on a personal computer (Webmail, Outlook, Eudora) either at home or in the workplace, the use of a virus scanner that will

inspect messages before they are read is strongly urged. Be highly suspicious of any unsolicited messages that contain attachments, with file types of .exe., .com, .bin and .vbs where the sender, subject line, or content seem out of place.

(6) Court order or law enforcement investigation may require the examination and release of any document, including electronic files such as e-mail. Colorado law provides that communications of College personnel that are sent by e-mail may constitute "correspondence" and, therefore, may be considered public records subject to public inspection under Colorado's Public Records Act, C.R.S. 24-72-203. However, e-mail messages produced or stored using state-owned equipment or software generally are excluded from the definition of "records" subject to the provisions of the State Archives and Public Records Act, C.R.S. 24-80-101, et seq. [<http://64.78.178.125/cgi-dos/statdspp.exe?L&doc=24-80-101>] Also, e-mail of students may constitute "education records" subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). The College may access, inspect, and disclose such records under conditions that are set forth in the statute.

When a person affiliated in any way with the College is involved, IT will act only under the specific instructions of a member of the College Attorney's office to ensure that individual rights, including rights to privacy and due process, are maintained.

(7) MSCD employees and business associates may, under certain conditions, have e-mail files accessed by others when it is related to departmental functions. A special condition exists for a staff employee or business associate who receives e-mail associated with College business functions and where, in that person's absence, a supervisor or others in the department needs to have access to the e-mail. IT must continue to maintain the privacy of e-mail but on authorization from the Department Head or Dean may locate and copy specific messages. No person outside IT may review the entire contents of an account's system mailbox without authorization by the College Attorney.

(8) Mail moved by the account holder outside the e-mail system becomes personal files covered by other policies and procedures. Note that e-mail downloaded to files on a personal computer or outside of the MSCD e-mail system is covered by other policies and procedures. Those files on a personal computer are outside the system management of IT.

(9) IT administers the campus e-mail system in a manner consistent with the system's importance for campus communication and the need for privacy of e-mail messages. In the process of administering the e-mail system, certain members of the IT staff may have access to the contents of certain e-mail messages. Furthermore, information about the contents of e-mail must not be

communicated to other members of the IT staff unless required to administer and support the system, and may not be communicated to anyone outside IT without the approval of the College Attorney (with the exception noted in (7) above).

(10) Although normally fast and reliable, delivery to on-campus e-mail addresses is not guaranteed. There is no assurance that the recipient will examine a particular message, nor can confidentiality be absolutely guaranteed. IT can provide advice on how to use additional procedures and software with the system when higher levels of security and confirmed delivery are required, for example with job applications or job searches.

(11) There are no assurances about the handling of e-mail received from or sent to addresses outside MSCD. Organizations managing e-mail systems elsewhere on the network may or may not have policies similar to those described here. Many are known to consider e-mail the property of the organization, subject to examination. Be aware of this possibility when you correspond with those elsewhere on the network. While IT may be able to provide some advice, MSCD has no direct influence on the handling of e-mail anywhere outside the local network.

(12) Some information about personal mail use is not confidential because of the way computer systems operate. Depending on how a person uses e-mail, the following information can be seen by other people: 1) The fact that a person is running a mail application. 2) The account to which mail is being addressed. 3) The size of the account's mailbox (mail waiting to be read). 4) The date and time mail was last read.

(13) The administrators of MSCD's e-mail facility may, within certain limits, block e-mail (including external, unsolicited, bulk e-mail --"spam"). The annoying, potentially resource intensive, and sometimes offensive nature of unsolicited bulk e-mail being sent by commercial or quasi-commercial organizations may require MSCD's e-mail administrators to block receipt of mail from some locations on the Internet. This blocking action is permitted if justified and where such blocking minimizes the likelihood that legitimate e-mail to MSCD account holders will be blocked as well. E-mail administrators are not permitted to use the content of the message or of the subject line in the mail heading to block or divert delivery of any message, except to block e-mail containing spam, computer viruses (or similar destructive content).

(14) The account holder must maintain password security. E-mail addressed to an account is delivered to a mailbox file that can be accessed through a variety of computer programs (e.g., Outlook, Pine, Webmail, Netscape, Eudora) under account password control. The account holder is responsible for maintaining strict confidentiality of that password, as described in the general statement on computer ethics and responsibilities.

(15) The account holder is expected to manage all mail delivered to that account. It is the responsibility of the account holder to manage her/his e-mail by suitably disposing of mail in the account's Inbox folder (deleting messages, moving messages to personal folders on the e-mail server, or moving them to a PC). Managing e-mail also requires account holders to suitably control the automatic delivery of messages from services such as mailing lists (e.g., Listserv).

(16) Electronic storage for Inboxes is limited and the IT staff must ensure that sufficient space is available for the on-going delivery of new messages. IT will establish a maximum permissible Inbox folder size. When this size is exceeded, the entire Inbox contents may be moved to a new folder on the mail server, where it will be accessible by the account holder. An e-mail message notifying the account holder that this action has been taken will immediately be sent, providing information about where the e-mail has been placed.

(17) Electronic storage for personal mail folders is limited on the E-mail server. Students, faculty and staff each receive a portion of centralized storage space for personal e-mail folders. This allotment is given when the e-mail account is created for the first time and generally appropriate for most use. IT will double the initial amount upon request. Student requests for amounts beyond this require the support of a faculty member. Requests for more than twice the general allotment must be made in writing to the College's CIO.

(18) Unread Inbox messages will be deleted from the server 180 days after they were sent. Unread e-mail that remains in the Inbox folder creates processing overhead for the post office mail server. Unread e-mail that resides in the Inbox folder is not archived during system backups. Unread e-mail messages in personal folders (moved from the Inbox) is not subject to deletion and is archived as part of normal system backup processing

(19) The accumulation of a large volume of mail in an account's Inbox may require IT to take management action. If an account receives a volume of e-mail that causes network degradation, mail processing slow downs, storage problems; IT will take actions to reduce the volume. In cases where, over a period of a week or longer, an account receives a large volume of mail and the account holder retains it in the Inbox, IT will begin a series of responses to safeguard the account holder's mail, protect performance of the e-mail system, and help the account holder gain control over the amount of mail being received. These are the response stages:

(a) Whenever the Inbox is moved to a personal folder, IT will send an informational message that will offer assistance and advice on how to manage the receipt of mail. It will alert the account holder to the need for him/her to take action in managing the account.

(b) IT will contact the person by phone or conventional mail to alert that person to the problem, to request that immediate action be taken, and to offer advice on

how to proceed.

(c) IT will request permission from the appropriate Dean or Vice President to deactivate the account.

(20) Extraordinary action may be required under specific constraints.

Certain circumstances may require IT to take extraordinary action in administering the e-mail system. This might be caused by system malfunction or malicious actions by an individual. IT must take steps to:

- (a) protect the privacy of mail,
- (b) protect the functionality of the e-mail system,
- (c) protect account holders from disruption of their use of the e-mail system.

Extraordinary action taken by IT to limit an individual's access to the system or to inspect and/or alter the contents of a mailbox is subject to review by the College Attorney.

(21) Group e-mail accounts-A group e-mail account is a single, MSCD e-mail address used by more than one person for conducting official business of the college.

A group e-mail account is different from a Lyris mail list or class-cluster mail list. The purpose of a group e-mail account is to provide an easy to understand functional name for the sender, provide a single depository (Inbox) for incoming e-mail, and to allow any group member to see, service, and respond to messages. The employee replying to an e-mail message can either do so anonymously through the group e-mail account or can forward the message to a personal account if a more personal reply is desired.

An e-mail alias is an alternative to a group e-mail account. Unlike a group account, an e-mail alias acts as a synonym for personal e-mail addresses. When a message addressed to an e-mail alias is received, the message is automatically forwarded on to one or more personal e-mail addresses. The sender is not aware they are addressing their message to an alias address. An e-mail alias does not have an Inbox nor can e-mail be sent from an e-mail alias. E-mail aliases are created and maintained by the System Administrator.

(22) Requesting a group e-mail account-Group e-mail accounts introduce special security concerns.

Unlike a personal account, which is used by only one person-harassing, threatening, or otherwise inappropriate e-mail cannot be traced to any one person when the message originates from an account used by multiple employees. Requests for group e-mail accounts must be made in writing to the Vice President of Information Technology (CIO) and include the following:
A description of the business function that will be served by such an account,
A description of the volume of messages that will pass through the account,
A description of the number of people and their job responsibilities who will share the account, and

The signature of the department head agreeing to take personal responsibility for the additional security risks presented by group e-mail accounts.

Notes: Portions of this document were taken from similar e-mail policies in place at Harvard Medical School, Colby College and the University of Colorado at Denver and Health Sciences Center.

VI. Use of Intel® LANDesk® Management Suite

I. Purpose:

With technology constantly changing, the Division of Information Technology is increasingly required to do more with fewer resources. One tool MSCD has invested in is Intel LANDesk Management Suite, which provides a powerful solution to this challenge. LANDesk can easily accomplish key tasks, such as distributing software applications and files, providing remote access to the desktop to fix problems, making purchase decisions based on hardware and software inventory, and keeping compliant with software licenses.

II. Policy:

Information Technology uses Intel Corporation's LANDesk utility software as part of the standard suite of software provided on all personal computers. This software provides four valuable functions: 1) it automates the computer hardware inventory process, 2) it continuously meters the standard suite of software to ensure compliance with licensing agreements, 3) it can be used to distribute software updates or problem fixes, and 4) only with the user's permission may it be used to remotely diagnose computer problems.

Function 1: Inventory

With the standardized desktop running Windows 2000 Professional, an accurate inventory of workstation and server assets is essential. With LANDesk, hardware and software inventory allows the administrator to see the configuration of every computer on the network. This comprehensive inventory does the following:

- Provides justification for upgrades
- Helps with hardware purchase decisions
- Assists in problem solving software issues
- Identifies and monitors any changes to existing desktop configurations
- Identifies specific hardware criteria as a requirement for software distribution

Function 2: Software Metering

Software metering tracks concurrent use of each software package and ensures MSCD is operating within its software license agreements. IT will only meter MSCD's standard desktop applications and will not attempt to meter the user's personal applications. Metered applications can reside either on a network server or on a local hard disk. Software metering can be used to:

- Track software usage for licensing compliance
- Document software usage to better manage site-licensing issues

Function 3: Software Distribution

Software distribution will allow applications to be scheduled for automatic delivery. IT will only maintain and update software that is part of the institution's portion of the hard drive. No attempt will be made to maintain the user's portion. Automatic distribution can be scheduled during off hours to avoid interfering with user productivity. Applications can be pushed to the client or even uninstalled. Software can even be distributed to users via the Internet or on floppy disk.

Function 4: Remote Help Tool

With the approval of the desktop user, Help Desk technicians can shorten problem resolution times and assist users without sending a technician to the user's computer, making it easier for them to achieve first-call problem resolution. Remote tools include:

- Access to desktop configuration information
- Remote access for problem-solving
- Diagnostics
- File transfers
- Remote Execute of Software tools (ex. Norton or ScanDisk)
- Remote reboot

VII. Computer Technology Procurement Policy [Desktop Upgrades, Software and Hardware & Network Hardware & Software]

I. Purpose:

To provide the College administrative and academic departments with the most appropriate desktop hardware and software, based upon the college computer and network architecture, and on software licensing restrictions and to achieve cost-savings available through site licenses and volume purchases.

II. Policy:

Administrative and academic departments must obtain approval from the appropriate funding authority for any technology purchase. Requests will not be processed without the approval of the account authority. Check with the vice president's office for the budget approval process in your area.

All purchases of desktop computer upgrades, hardware and software as well as network hardware and software for MSCD administrative and academic departments must be reviewed and processed through the Information Technology Administration Office to ensure compatibility with college computer and network architecture and software licensing restrictions. An IT technician will review and analyze the desktop equipment for which the request is being made to insure the appropriate hardware or software is identified and that any software requested will not interfere with existing software or with the College system. Only software with the appropriate, official licensing will be installed on College desktop computers. Employees may not install software that is not authorized by the software license. [See MSCD **Administrative Policy #4**, "[Copying Computer Software.](#)"]

Note: Equipment and software procurement for student laboratories is addressed in a separate policy.

Approved by President's Cabinet November 15, 2000

VIII. Contract Personnel Service for Information Technology Work

I. Purpose:

The purpose of this policy is to insure the Division of Information Technology is able to fulfill its stewardship role in regards to both data assets and technology infrastructure. The Division of Information Technology hires both individuals and companies to provide software, hardware and technology analysis when demand for service outstrips IT's ability to deliver those services with existing personnel. In addition, other departments in the College may engage the services of consultants to perform Information Technology related activities, such as analysis, and software development.

When IT retains such services, IT directly oversees the work of the service provider, thereby ensuring all work is according to College policy, respects privacy and security concerns, follows the institution's technology architecture, and can be maintained once the service provider is no longer under contract. When other departments retain such services, there is often no guarantee of such monitoring by technically trained personnel.

II. Policy:

All purchases of contract and personnel services related to Information Technology consulting, software development, systems analysis, or other IT activity that could impact either the College computer network or its administrative systems, must have prior approval from the Vice President of Information Technology. The work performed by that contractor must be performed in accordance with current practices within the Division of Information Technology. In the event the Vice President of Information Technology disagrees with the planned contract services, the Vice President will inform the MSCD employee within three days with the reasons for disapproval.

IX. Guidelines for Electronic Mailing Lists by Major

I. Purpose:

The Division of Information Technology has developed e-mail lists for each group of majors in each department within the Schools of Business, Letters, Arts and Sciences and Professional Studies. Non-degree seeking students and undeclared majors are assigned to the list for the Advising Center by the Director of the Advising Center. These lists will be populated from Banner on a nightly basis, effective mid-September 2001.

In order for these electronic mailing lists to be useful, students must be encouraged to declare a major so that they do not miss vital communication emanating from their departments. Moreover, students must be encouraged to set-up their MSCD e-mail account so that they can receive e-mail messages.

With over 50 majors and e-mail lists being developed, it is important for IT to implement a consistent format with consistent guidelines for all departments. IT will provide training and simple instructions to all department chairs and deans to enable them to manage their electronic mailing lists easily.

II. Policy:

Subscription to each list will be mandatory to ensure a means for one-way communication from the department to its majors. In other words, students who are majors will not be able to "unsubscribe" from the list if he or she is a major. If a student changes majors, his or her name will remain on the original major list as well as having his or her name added to the new major list. However, instructions will appear at the bottom of each e-mail the Chair sends giving students instructions about how to "unsubscribe" if he or she is no longer a major. In other words, students will continue to receive e-mails from each department in which they have declared a major unless they take action to remove their name from the list. Majors who attempt to "unsubscribe" will be automatically added back by Banner overnight.

By default, students will not be able to respond back to the list. If the Chair wishes to receive individual feedback from the department's majors, then the Chair should include his or her e-mail address in the text of the announcement and solicit comment.

The Dean of the respective department will be included by means of a copy on all communication to the mailing list so that he or she receives the same communication that each major in that School receives. However, the Chair will control the mailing list for each department. Only the Chair and Dean will have authority to send communications to the majors on the list and to add or delete majors from the list. The right to post to these lists is not to be shared with any other individual or entity without prior clearance by the College Attorney. In the

event a College official wishes to post to a mailing list, the request must be put in writing and given to the Dean of the respective School for review. The Dean, in consultation with the Chair, has the authority to deny such a request. If the Dean approves the request, a copy should be kept on file in the Dean's Office for future reference.

X. Use of Napster and Similar Software Programs

I. Purpose:

A number of applications are used to search for and share MP3 music, video and image files-such as Napster, KaZaA and Gnutella. This software scans the World Wide Web for other computers using these software programs and then exchanges files automatically. The nature of this software and the way it works presents MSCD with a number of problems:

- Sending and receiving MP3 and other media files consumes large amounts of the campus' limited and expensive network bandwidth.
- Most of the files in question are copyrighted material. It is illegal under Federal law (Title 17 of the US Code, and more recently the Digital Millennium Copyright Act, 105 PL 304) to distribute copyrighted material in this fashion.
- Workstations with Napster or Napster-like software may function as public file servers and allow people to browse private or confidential information in an employee's data files.
- Some of these applications are known to install "spyware" programs that periodically "phone home" information about the computer and the computer user's patterns of network use.

II. Policy:

Faculty, staff and students are prohibited from installing or running Napster, KaZaA, Gnutella, or other software programs with similar functions on computers owned by MSCD or installed on MSCD's network. If a faculty or staff member has a need to use one of these software products for an academic or instructional purpose, he or she should inform Information Technology by sending an e-mail to helpdesk@mscd.edu so that Internet access is not blocked.

For additional information please see these resources:

<http://www.educause.edu/issues/napster.html>

<http://www.uchicago.edu/docs/policies/eaup/napster.html>

<http://www.utsystem.edu/OGC/IntellectualProperty/napster.htm>

<http://www.luc.edu/infotech/cease/p2p-file-transfer.html>

XI. Web and Internet Technology Policy

I. Purpose:

MSCD recognizes the scope of the World Wide Web and the importance of Internet technology in the dissemination of information both internal and external to the College. MSCD is committed to the development and support of quality content and expert delivery of content over MSCD web.

Such a far-reaching medium requires the combined resources of IT, College Communications and individual MSCD departments. This policy has been developed to assist in the management of the MSCD Web and Internet resources.

II. Policy:

Responsibilities

It is the responsibility of an MSCD web developer to read and meet the terms and conditions of the MSCD Web Style Guide (currently being developed by Institutional Advancement) and the Responsible Use of Information Technology Resources Policy. All questions or requests regarding this policy can be e-mailed to helpdesk@mscd.edu.

Information the College Gathers:

MSCD Web servers generate temporary logs that contain the following information:

- Internet address of computer being used
- Referring web page
- Web pages requested
- Date and Time
- Browser used
- NID (unique person identifier for Banner services only)

The log data is used by system administrators and web content managers to tune the web site for efficiency and is not ordinarily associated with specific individuals. See Responsible Use of Information Technology Resources Policy for further information.

Summary reports produced from the logs help web publishers determine what pages are most popular. For example, the aggregate reports can show each page accessed and how many times it was viewed. The reports can also show what times of the day and what days of the week are most popular and where the web users are accessing the Internet from.

Use of Cookies:

MSCD web servers use cookies in different ways. Cookies are small pieces of

data stored by the web browser. Cookies are often used to remember information about preferences and pages specific users have visited. For example, when visitors access some sites on the web they might see a "Welcome Back" message. The first time a visitor accessed the site a cookie was probably set on his or her computer; when he or she returned, the cookie was read again. Visitors can refuse to accept cookies, can disable cookies, and can remove cookies from their computers. Please refer to your web browser manual for instructions on doing this.

MSCD's Student Information System may use cookies so users do not have to repeatedly enter user names and passwords when visiting different areas of the student information system. This login process shall use Secure Socket Layer (SSL), so the user name and password are encrypted between the web browser and our web server.

Some Web servers within the institution may also use cookies to retain user preference information. This information may not be shared with external third parties.

E-commerce & Revenue Generation:

Several sites within the College's web system enable students to pay for products or services online with a credit card. Unless otherwise noted on the website, these transactions shall be encrypted using SSL technology. Confidential information entered during the transaction may be used only for the purposes described in that transaction, unless an additional use is specifically stated on that site.

Web Security and Data Recovery:

The system administrators of the servers on which College sites exist will provide reasonable protection from accidental loss, tampering, or unauthorized access. The creator of the web site, however, is responsible for protecting his/her own sites by keeping passwords secret and changing them regularly; as well as monitoring the security of any executable code (CGI scripts, server side includes, JavaScript, etc.) placed on a College server.

The system administrators reserve the right to monitor all software placed on campus servers for potential security threats, and remove this software as necessary. See [Responsible Use of Information Technology Resources Policy](#) and the [Use of Intel® LANDesk® Management Suite Policy](#) for further information. Web site creators are also responsible for maintaining personal backup copies of their sites to protect against loss or damage.

Any transactions that require secure communications (such as in the use of Social Security, PIN, or credit card numbers over the internet), must receive the approval of the department chair and an IT representative to ensure that the

transmission, storage, and use of such data meets standards for security and privacy, such as using SSL.

As mentioned previously, web site creators are responsible for maintaining personal backup copies of their sites to protect against loss or damage. However, should the need arise, recovery of data from the tape backup library can be requested through the IT Help Desk at 303-556-8325 or by e-mail at helpdesk@mscd.edu.

XII. Kiosk Idle Loop Usage

I. Purpose:

Metro State owns and services four kiosks located in various places on campus. Students can utilize these kiosks to access grades, transcripts, class schedules and to register for classes. While the kiosks are not in use, a screensaver referred to as the "idle loop" is displayed on the kiosk. This screensaver displays a new image every three seconds and continues to cycle through the loop until a student accesses the kiosk. Modifying the idle loop requires an IT staff member to spend between two to three hours updating a movie file. Since the implementation of the kiosks, the idea of using the "idle loop" for commercial and departmental advertising purposes has been raised. Therefore, the following policy has been developed.

II. Policy:

Due to the limited space and time required to update the kiosk "idle loop" as well as the brief period in which each screen is displayed, neither commercial nor departmental advertising will be permitted on the kiosks. The Division of Information Technology, with the advice of College Communications, will update the kiosk idle loop at the beginning of each semester and on special occasions, with approval of the IT Administration.

Every department, club and organization has the ability to post events to the campus-wide events calendar, which in turn is accessible through the kiosks. Requests for access to post to the campus-wide events calendar should be sent to the IT Web Manager at webmgr@mscd.edu . Departments may also wish to utilize the digital announcement board located in the Central Classroom building for advertising special events and promotions. The Department of Business Services manages the use of the announcement board. Please contact them at: (303) 556-4646.

MSCD ADMINISTRATIVE POLICY (#34)

XIII. Electronic Communication Policy

I. Purpose:

Electronic communication (i.e. e-mail and personal portal announcements) is a rapid, efficient and cost-effective form of communication. Consequently, reliance on electronic communication is expanding among students, faculty, staff, and administration at Metropolitan State College of Denver (MSCD). Because of this increasing reliance and acceptance of electronic communication, forms of electronic communication have become in fact the means of official communication to students, faculty and staff within MSCD. This policy acknowledges this fact and formally makes electronic communication an official means of communication for the College.

Implementation of this policy ensures that all students, faculty and staff both full-time and part-time will have access to these critical forms of communication. All current students, faculty and staff have an account within the campus portal providing access to e-mail and official announcements.

II. Scope:

This policy also provides guidelines regarding the following aspects of electronic communication as an official means of communication:

- College use of e-mail and personal portal announcements;
- Assignment of student, faculty and staff portal accounts, which include e-mail addresses;
- Student, faculty and staff use of and responsibilities associated with assigned portal accounts and e-mail addresses; and
- Expectations of electronic communications between students, faculty and staff.

III. Policy:

1. College use of electronic communication
E-mail and personal portal announcements are an official means of communication to students, faculty and staff within MSCD. Therefore, the College has the right to send communications to students, faculty and staff via e-mail and personal portal announcements and the right to expect that those communications will be received and read in a timely fashion.
2. Assignment of portal accounts which includes e-mail addresses
Every current student, faculty and staff member are automatically provided with a portal account, which includes an assigned e-mail address. The e-mail address assigned to each student, faculty and staff member, as recorded in the Banner System, will be the official e-mail address of record for communications with students, faculty and staff. Students, faculty and

staff members will be deemed to have read e-mails sent to that address. Constituents are also responsible for reading any official announcements delivered through personal announcements channel on each user's portal home page.

3. Expectations regarding use of portal announcements and e-mail
Students, faculty and staff are expected to check personal portal announcements and their official Metro e-mail address inbox on a frequent and consistent basis in order to stay current with College communications. Students, faculty and staff have the responsibility to recognize that certain communications may be time-critical.
4. Educational uses of portal services and e-mail
Faculty members will determine how portal services and e-mail will be used in their classes. It is highly recommended that if faculty members have e-mail requirements and expectations, they specify these requirements in their course syllabus.
5. Appropriate use of portal services, including e-mail
 - a. All MSCD constituents are expected to adhere to the College's Responsible Use of Information Technology Resources Policy. See <http://www.mscd.edu/~infotech/policies/manual/itpolicy2.htm>
 - b. All use of e-mail, including use for sensitive or confidential information, will be consistent with the Metropolitan State College of Denver Administrative Policy Manual on Use of Electronic E-mail. See <http://www.mscd.edu/infotech/policies/>. Policy Title: Electronic Mail Policy and Procedures Principles, Policies, User Responsibilities, and Information, and Information Technology (IT).
 - c. E-mails pertaining to identified students are records protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). Employees have a responsibility to ensure that they are sent only to the subject student, or to college employees who need to see the e-mail to do their jobs, in the absence of the student's written permission to disclose the information to others.
 - d. Whenever the law or College procedure requires a different form of communication, that form will be used even though e-mail may also be sent. For example, formal notices in hard copy may be required under procedures relating to personnel actions, such as reduction in force, dismissal, discipline, or correction.

IV. Procedures:

The IT Policy Committee will oversee and make recommendations for revision of this policy as needed. Changes will be authorized by the approval of the President.

V. Responsible Organization:

The IT Policy Committee will be responsible for this policy.

MSCD ADMINISTRATIVE POLICY #35

XIV. Broadcast Messages (Voice mail and E-mail)

I. Purpose:

Metropolitan State College of Denver is committed to the use of broad-based electronic communication to improve the efficiency of communication, to reduce environmental (paper) waste, to improve the College's ability to provide targeted services, and to help build community.

The purpose of this policy is to keep the volume of messages at a reasonable level, focused on College business, and to ensure that electronic lists remain a reliable means of communication at Metropolitan State College of Denver. "Junk messages" broadcast to a wide audience are annoying and may defeat the goal of effective communication using these technologies. They also place undue burden on personnel, server and network resources.

Broad-based electronic communications include broadcast voice mail ("audix") messages and e-mail postings to *involuntary* and *voluntary* mailing lists.

II. Scope:

This policy is intended to cover group electronic communication sent via the College voice and e-mail systems. This policy applies to all students, faculty and staff at MSCD.

III. Policy:

Voice mail and e-mail that is sent using College-provided systems and services is intended for use for official College business or College-related purposes only. Lists may not be used by individual employees or students to send mass messages of a personal, commercial, fundraising nature, or to advocate for or against a proposition or candidate on the ballot in a state or local election. (See Section IV.: Administration & Implementation.)

A. Involuntary Global and Group E-mail Lists

When the College sends broadcast e-mails, the mailings will be directed to a user's College-provided e-mail account (username@mscd.edu). Faculty, staff and students are responsible for reading the information contained in all official e-mail messages sent from the College and following the instructions they contain. Failure to use the College's e-mail resources is not an acceptable excuse for failure to comply with directives sent by the College via e-mail. For more information, see the MSCD "Electronic Communication Policy" at <http://www.mscd.edu/policies/ecommunications.htm>.

1) *Lyrus Lists*: [All-faculty, All-classified, All-administrators & All-adjunct] Only members of these lists may post to the lists. Permission for non-members to use

automated, global mailing lists must be obtained from the appropriate Cabinet Officer or his/her designate or the Office of College Communications. If approved, the appropriate Cabinet Officer or designee must post the message.

2) *Portal E-mail and Portal Announcement Lists*: The President, the members of the President's Cabinet, Deans and their designees have the authority to send targeted mailings through MetroConnect to segments of the College community through specialized involuntary electronic mailing lists created from College held data.

When mailing to these lists:

- Cabinet Officers and their delegates are responsible for the content of messages posted to involuntary automated lists. Agents who have been given the authority to post messages to involuntary automated lists by a cabinet member may not further delegate this authority without the express written permission of the appropriate Cabinet Officer.
- Cabinet Officers are responsible for ensuring that the appropriate procedures are in place to review and approve messages prior to posting.
- Those officials with the authority to post to involuntary e-mail and portal announcement lists are responsible for ensuring that their designees receive adequate training, supervision and guidance regarding the appropriateness of content and the use of proper techniques for posting messages.
- Records of broadcast messages must be kept, including sender, recipients and a copy of the message itself.
- Replies will be to the sender or list members only.

B. Voluntary Portal Groups and Channels

For departments that need to send notices and information related to area-, department- or discipline- specific events and announcements, communication tools are available within MetroConnect. These tools include Groups and Channels. Both options are voluntary and provide users with the ability to opt-in or out of the group e-mail list or to subscribe to the channel. Faculty, staff and eligible student organizations may use voluntary groups or channels within the portal. The procedure for requesting the creation of a group or channel can be found at <http://www.mscd.edu/policies/metroconnect/contentguidelines.pdf>. For training documentation on portal Groups, see <http://www.mscd.edu/metroconnect/helpdocs/>.

C. Voice Messages

The Office of College Communications must approve and transmit any and all broadcast messages via campus phones.

D. Emergency Situations

In emergency situations centralized communications are necessary to ensure that accurate information is being disseminated. During such times all broadcast voice and e-mail messages will be coordinated through the Office of College Communications.

IV. ADMINISTRATION AND IMPLEMENTATION:

Accepted Use

Voice mail broadcasts and global mailing lists may be used for announcements and messages concerning:

- emergencies, health and safety;
- College-wide events and deadlines, and notification of the availability of services and/or facilities, aggregating messages where possible;
- matters of policy or processes, including changes in campus policies, procedures, organizations, or departments; or
- timely communication that has direct impact on members of the College community.
- Approved college publications such as @Metro and Metro in the Media.

Appropriateness

As a general principle, the larger the number of recipients, the greater the need for establishing that the recipients will find a particular message useful. Questions about appropriateness of a message or audience may be addressed to the appropriate area administration (e.g., campus Registrars for student data). In addition, voice messages require approval from the Office of College Communications. Points to consider when sending a broadcast message include:

- Ensure that the subject of the message is relevant to the audience, is of interest and not repetitive, and relates to list members. (e.g., do not send a message to all employees if the message is applicable only to faculty and students).
- Ensure that the message is clearly worded and not offensive to the recipient.
- Ensure that the message is significant enough that it would be sent even without the ease of e-mail or voicemail. For example, is the message one that would be printed and mailed, or produced in "flyer form" and posted or distributed?
- Consider sending the message through representative groups. For example, in sending a message to Faculty, contact the Faculty Senate, the Academic Vice President, School Dean or Department Chair.
- Consider more efficient mechanisms for dissemination of the information, such as the MetroConnect Event Calendar.

Inappropriateness

It is inappropriate to:

- Send mass messages of a personal, commercial or fundraising nature or which advocate for or against a proposition or candidate on the ballot in a federal, state county, city, municipal, school board or special district election.
- Forward chain letters or electronic “petitions,” or to ask recipients to forward messages.
- Send anonymous mailings.
- Solicit support (financial or otherwise) for charity, political parties or candidates, or other special causes not connected with a College effort.
- Send unverified public service announcements (such as virus alerts, unsafe products, lost and found, items for sale, giveaways, etc).
- Include attachments if the information is or can be posted on a College Web site.

V. DEFINITIONS AND EXAMPLES:

A. ***Broadcast voice mail messages:*** A broadcast (“audix”) voice mail is one that is sent to everyone on the campus phone system.

B. ***Involuntary E-mail Groups and Mailing Lists*** are created from College-held data about students, faculty, staff and others. These lists may include, for example, all members of the College community or subsets, such as all faculty, all students, all faculty in a School, students in a particular major or course, etc. Recipients cannot elect to be excluded from these mailings. Two types of groups or lists are available:

1. **Lyris Lists:** Information Technology (IT) maintains automated mailing lists for large segments of the College community such as all-faculty, all-classified staff, all-administrators and all-adjunct faculty. Only list members and designated College administrators may post to these lists. List members may not post messages on behalf of non-members.
2. **Portal E-mail and Announcement Lists:** Certain college agents have the ability to post to mailing lists for targeted populations. These agents include the President’s Cabinet, Executive Officers, the Deans, and their designees, as well as the Registrar, Financial Aid Officers and the Human Resources Office.

C. ***Voluntary Portal E-mail Groups and Channels*** are composed of members (students, faculty and staff) who have chosen to subscribe to such groups or channels within MetroConnect. Postings are directed to all list members. Faculty, staff and eligible student organizations may use voluntary groups or channels

within the portal. There are two alternatives for voluntary e-mail and announcement distribution.

1. Portal Groups (See <http://www.mscd.edu/metroconnect/helpdocs/>).
2. Portal Channel

For information on how to request a portal group or channel go to:
<http://www.mscd.edu/policies/metroconnect/contentguidelines.pdf>)

VI. ENFORCEMENT

The MSCD HelpDesk should be notified of inappropriate mail (send e-mail to helpdesk@mscd.edu or call 303-556-8325). The matter will be referred to the appropriate College official.

Electronic mailing list use is subject to the terms of Metropolitan State College of Denver's Responsible Use Policy (see: <http://www.mscd.edu/~infotech/policies/manual/itpolicy2.htm>), as well as other applicable College policy, and Federal or local statutes. Use of mailing lists is also subject to review by internal audit.

VII. APPROVAL

Approved June 16, 2004 by the MSCD President's Cabinet.

[This policy will be reviewed as needed, but particularly when there are significant changes in voice or e-mail systems or policies, and/or underlying information systems or services.]

Note: Portions of this document were taken from similar policies in place at Georgetown University.

XV. Ad Hoc access to BANNER Databases

I. Purpose:

To establish policies and procedures for granting Ad Hoc access privileges to the BANNER database.

II. Scope:

These policies affect all users with access to any BANNER database.

III. Introduction:

Metropolitan State College of Denver (MSCD) places a premium value on the data collected, created by and used by the institution. This data is vital to the on-going operation of the College. Everyone associated with the College has an obligation to protect this vital asset from unauthorized or inappropriate access, unauthorized or inappropriate use and, unauthorized or inappropriate alteration or destruction.

The College recognizes and values the privacy of its students and employees. Everyone associated with the College has an obligation to protect, within reason, the privacy of students, employees and College associates.

The principle of least privilege states that a user (or program) is not given access to more data, or given more access privileges, than is necessary to perform their duties. This requires a good understanding of what data a user needs to access, and what access privileges (read/insert/update etc...) are necessary, for them to be able to perform their assigned duties.

The BANNER forms do an adequate job of controlling a user's access to BANNER data. However, there are other tools that can be used to access BANNER data. Tools such as MS Access and SQL*PLUS bypass many of the security features provided by BANNER forms. The statements listed below define policies to govern the granting of Ad Hoc access privileges to BANNER data.

IV. Definitions:

Ad Hoc access: Using applications, such as SQL PLUS or MS ACCESS, that are capable of dynamically querying data from the BANNER database.

BANNER module owner: The individual responsible for the administrative oversight of a given BANNER system (i. e. Student, Finance, Financial Aid, etc...) and ultimately responsible for the data within said system.

Oracle role: A technical security mechanism used to define access privileges to specific data within the BANNER database.

V. Policy Statements:

1. BANNER users, and programs accessing BANNER data, will be given access to the Oracle Role that most closely matches the data which is necessary for them to perform their assigned duties. By default, BANNER users will not be given "ad hoc" query privileges. No BANNER user will be permitted to query all BANNER data.
2. Each BANNER module owner is responsible for determining which database role a user needing ad hoc access to the data within their BANNER module, should be given.
3. Users of the BANNER system and data are responsible for complying with all College policies regarding privacy, security, and the appropriate use of BANNER data and other College resources. Managers and supervisors are responsible for insuring that their employees comply with said policies and procedures.
4. The inserting, deleting or updating of BANNER data will only be performed using applications developed and installed by SungardSCT or the Department of Information Technology for that express purpose. Applications developed by 3rd parties may be certified for such use by either SungardSCT or Information Technology.
5. Applications that were not developed or certified for use by SungardSCT or the Department of Information Technology are considered to be "ad hoc". Ad hoc applications will be restricted to read only (select) access. The use of ad hoc programs must be compliant with these and other applicable policies.
6. These policies and ensuing procedures will be applied retroactively. No BANNER user, application program or system will be exempted from or "grandfathered" under these policies and ensuing procedures.

VI. Guidelines:

A conservative approach is recommended when assigning BANNER access privileges. Access privileges should be commensurate with an employee's training, knowledge, skills, degree of supervision and, their assigned duties. Supervisors should periodically review their employees' access privileges to ensure the access is appropriate for their assigned duties. The department of Information Technology and Human Resources should be notified immediately when any employee leaves employment of the Institution or relocates to another department.

VII. Remedies for non compliance:

Failure to comply with these policies may result in one or more of the following actions: a) suspension of access to the network, b) when appropriate, disciplinary action in accordance with the Metro State Handbook for Professional Personnel

or State Classified Personnel Rules, c) when appropriate, initiation of civil or criminal proceedings.

Approved January 30, 2005

XVI. BANNER Security Policy

I. Purpose:

To establish policies, procedures and guidelines for accessing and using the College's BANNER data.

II. Scope:

These policies affect all users with access to any BANNER data.

III. Introduction:

Metropolitan State College of Denver places a premium value on the data collected, created by and used by the institution. These data are vital to the on-going operation of the College. Everyone associated with the College has an obligation to protect this vital asset from unauthorized or inappropriate access, unauthorized or inappropriate use, and unauthorized or inappropriate alteration or destruction.

Metropolitan State College of Denver recognizes and values the privacy of its students and employees. Everyone associated with the College has an obligation to protect the privacy of students, employees and College associates.

Metropolitan State College of Denver recognizes the need for institutional data to be shared in a timely, efficient and secure manner amongst various departments with a demonstrable official need for the data.

Metropolitan State College of Denver will take all reasonable and prudent measures to protect the confidentiality, integrity and availability of its information processing assets. Such measures will, in addition to technical and physical controls, include administrative policies, procedures, guidelines and training.

IV. Definitions:

BANNER Managers: A committee comprised of BANNER module owners, department managers, end-users, and IT personnel responsible for coordinating the development, implementation, maintenance, and general stewardship of the SunGard SCT BANNER information system at Metropolitan State College of Denver.

BANNER module owner: The individual responsible for the administrative oversight of a given BANNER system (i. e. Student, Finance, Financial Aid, etc.) and ultimately responsible for the data within said system.

V. Policy Statements:

1. BANNER data is the property of Metropolitan State College of Denver. Access to BANNER data is restricted to authorized personnel only. Unauthorized access is prohibited.
2. BANNER data will be used for official College business only. Specific non-College business use of BANNER data may be authorized under other official College policy. Unless specifically permitted by another official College policy, the use of BANNER data for personal gain or curiosity, or another's personal gain or curiosity, is prohibited.
3. Persons, and processes, accessing BANNER data will uphold the confidentiality and privacy of individuals whose data they access and observe any laws, regulatory requirements, policies and ethical restrictions that may apply with respect to their accessing, using or disclosing such information.
4. Persons, and processes, with access to BANNER data, regardless of its form (electronic or print), will insure that all reasonable and prudent measures are taken to protect the data from theft and unauthorized or accidental viewing, copying, downloading, modification or destruction. The data must be protected while in use, in transit and in storage. The Department of Information Technology is to be notified immediately in the event the security of any BANNER or other administrative data is compromised.
5. Anyone in the service of the College, with a genuine business or educational need, may be authorized to access the BANNER data necessary to perform their duties. An individual's access to BANNER data will be removed when the individual leaves the service of the College or during an extended absence. Supervisors are to notify the Department of Information Technology (556-8325) and the Office of Human Resources (556-3120) immediately when an individual, including student employees, leaves their service or begins an extended absence.
6. BANNER Module Owners have the sole authority to authorize access to the data within the modules they administer. Module Owners are encouraged to use the principle of least privilege when authorizing access to their module data.

VI. Reporting Violations:

Any suspected violations of these policies, or unauthorized access to computing resources, or any other condition which could compromise the security of BANNER data or other college computing resources must be reported to the Department of Information Technology, Security and Disaster Recovery Coordinator, <http://www.mscd.edu/~infotech/security/>, (303) 556-8325.

VII. Remedies for non compliance:

Failure to comply with these policies may result in one or more of the following actions: a) suspension of access to the network for the individual or unit violating the policy, b) when appropriate, disciplinary action ranging from warning to

termination and (for students) expulsion from the College, depending on circumstances, in accordance with applicable policies and procedures, c) when appropriate, initiation of civil or criminal proceedings.

VIII. Authority:

The Office of the President grants authority to the Vice President of Information Technology, in conjunction with the BANNER Managers committee, to oversee compliance with this policy. The BANNER Managers will review this policy annually and recommend revisions as necessary.

IX. Related documents and policies:

Family Educational Rights and Privacy Act

<http://www.mscd.edu/academic/catalog/section1c.htm#ferpa>

Responsible Use of Information Technology Resources

<http://www.mscd.edu/%7Einfotech/policies/manual/itpolicy2.htm>

Ad Hoc access to BANNER Databases v2.0

<http://www.mscd.edu/~infotech/security/requestforms/AdHocAccessPolicy.htm>

X. APPROVAL

Approved May 11, 2005 by the MSCD President's Cabinet.

[This policy will be reviewed as needed, but particularly when there are significant changes in voice or e-mail systems or policies, and/or underlying information systems or services.]

XVII. Use of Wireless Networking Devices at Metropolitan State College of Denver

I. Purpose:

To establish policy regarding the use of wireless devices on the college's network.

II. Scope:

This policy applies to all areas of Metropolitan State College of Denver.

III. Introduction:

The college's computer network (both wired and wireless) exists to support the college's educational mission and related business functions. The network provides access to information and other resources that are important to all of the college's educational and business units. Some of the information consists of confidential, personal data about members of the College community. It is very important that the network provide continuous access to, and reasonable security for, the confidential data and other resources on which the entire community depends.

The deployment of unauthorized or improperly configured wireless devices poses a serious threat to the security and stability of the college's network.

The Department of Information Technology (IT) is responsible for building, maintaining and securing the college's network infrastructure (both wired and wireless).

This policy ensures the security and stability of the college's computing network and the data contained within.

IV. Policy Statements:

1. The Department of Information Technology has the sole responsibility and authority to deploy wireless networking equipment to be used by members of the college community.
2. The Department of Information Technology will coordinate the deployment of Metro State's wireless networking equipment through the Auraria Cooperative Technology Committee (ACTC).
3. Wireless networking approved and provided by the Department of Information Technology or a similarly authorized department of another Auraria institution has priority over other wireless networks. Previously deployed wireless networks that are not so approved and deployed may be shut down. Information Technology will make every reasonable effort to provide the Department with the level of service that they are accustomed.

4. Any other MSCD employee or administrative unit wishing to deploy a wireless network must submit a request to the Department of Information Technology who will evaluate the proposal and if appropriate, carry the request to ACTC for their approval. Criteria for the evaluation will be posted on the IT website.
5. Any MSCD employee or unit deploying an approved wireless network is required to:
 - a. Assign the static IP address, issued by IT, to the wireless access point.
 - b. Use strong encryption approved by IT.
 - c. Not advertise or promote their wireless network as being available for general use by the campus community unless such access is approved by ACTC.
 - d. Ensure that access to their wireless network is restricted to those users authorized to use their wireless network through means approved by IT.
 - e. Ensure that usage of their wireless network is congruent with published college policy.
 - f. Consult with IT before relocating their access point to another location.
6. The Department of Information Technology may temporarily disconnect, without prior notice, any wireless access point that is endangering the security of the college's network, malfunctioning, or being used in violation of published college policy. The Department of Information Technology will make a reasonable effort to work with the department hosting the device to resolve the security concerns before permanent disconnection. In all cases, the Department of Information Technology will make every effort to notify the operator of the device and the department head immediately.

V. Remedies for non compliance:

Failure to comply with these policies may result in one or more of the following actions: a) suspension of access to the network for the individual or unit violating the policy, b) when appropriate, disciplinary action ranging from warning to termination depending on circumstances, in accordance with the Metro State Handbook for Professional Personnel or State Classified Personnel Rules, c) when appropriate, initiation of civil or criminal proceedings.

VI. Authority:

The Office of the President grants authority to the VP of Information Technology to oversee compliance with this policy. The VP of Information Technology will review this policy annually and revise as necessary.

Approved by Cabinet: Tuesday October 5, 2004

Approved October 5, 2004

XVIII. IT Governance Policy

I. Metropolitan State College of Denver Statutory Mission Statement

Colorado law assigns the following mission statement to Metro State:

There is hereby established a college at Denver, to be known as Metropolitan State College of Denver, which shall be a comprehensive baccalaureate institution with modified open admission standards: except that nontraditional students who are at least twenty years of age shall only have as an admission requirement a high school diploma, a GED high school equivalency certificate, or the equivalent thereof. Metropolitan State College of Denver shall offer a variety of liberal arts and science, technical, and educational programs. The college may offer a limited number of professional programs. Metropolitan State College of Denver shall not offer graduate programs. (Colorado Revised Statutes, Title 23, Article 54, Section 101)

II. Metropolitan State College of Denver Operational Mission Statement

In December 2003, the Metropolitan State College Board of Trustees adopted an operational mission statement. The operational mission statement translates the statutory mission statement into a statement meant to guide the daily operations of the College and provide a more descriptive statement for planning purposes.

Metropolitan State College of Denver is a comprehensive, baccalaureate Degree-granting, urban, non-residential "College of Opportunity." With its modified open admission policy, the College welcomes students from all walks of life and circumstances, including all levels of academic preparation consistent with statutory guidelines, all conditions of economic and income status, all ages and all ethnic and cultural backgrounds. In addition to degree-seeking students, non-degree students seeking opportunities for continuing education are welcomed.

The College is a teaching institution where excellence in teaching and learning is accorded the highest priority. The College seeks to attract and build long-term relationships with a highly qualified faculty and staff with diverse interests and abilities. As partners in the College's fulfillment of its mission, faculty, staff and student participation through shared governance is encouraged and valued.

Student success, supported in a collegial atmosphere of academic freedom, is of paramount importance and all members of the College community seek to inspire students to strive for the highest level of future

achievement. The College seeks excellence in all programs and activities and evaluates the attainment of excellence utilizing measures focused on the knowledge, skills and understanding students gain during their educational experience with the College. A successful college experience enables students at Metro to achieve their specific educational goals.

The College offers programs and courses in the letters, arts, sciences, professional and business disciplines. The College is committed to a liberal arts foundation for all education by which each graduate develops the ability to communicate and reason effectively as a culturally and economically literate citizen in a multicultural, global and technological society. The College seeks to provide its programs and services to a diverse student body in an environment of quality, accessibility and affordability. Mutual respect, creative endeavor and scholarly inquiry, within and among all College constituencies, are expected.

The College provides students with an enriching education that leads to rewarding careers, prepares them for post graduate study, embraces the quality of their lives, and enables them to be well-educated, critically thinking citizens who contribute and participate in meaningful ways in community and civic life. Partnerships with the College's Foundation, Alumni Association, non-profit agencies and service organizations, corporations, businesses, civic and governmental agencies, as well as the community at large, assist the College in fulfilling its mission. Institutional priorities are established in accordance with the interests and needs of students, faculty, staff, employers and the citizens of Colorado.

III. Metropolitan State College of Denver Vision Statement

A vision statement is a succinct expression of the general direction the College intends to pursue in the context of its mission and the resources available to accomplish the mission.

As Colorado's "College of Opportunity," Metropolitan State College of Denver strives to be Colorado's leader in urban, public baccalaureate education by focusing its resources on quality, accessibility, affordability, and accountability.

Excellence in teaching and learning is the College's primary objective as it supports the educational goals of recent high-school graduates, transfer students, adult learners wishing to finish a baccalaureate degree and citizens intent on acquiring new skills or desiring to enrich their lives through participation in lifelong learning.

IV. Information Technology (IT) at Metropolitan State College of Denver Mission, Purpose, Value, and Vision Statements

Mission

- To enhance teaching and learning experiences with technologies by enabling timely, cost-effective and high quality delivery of state of the art computing and technology, through collaboration and participation with faculty, staff, and students.

Purpose

- To provide valued leadership, expertise and service in information technology to the Metro State community.

Value Statement

- We build relationships with colleagues and customers, practicing personal integrity, accountability and commitment to the college while supplying excellence in information technology.

Vision Statement

- IT aspires to provide exceptional technological solutions and services that foster personal creativity, opportunity for collaboration, flexibility and unfettered access to people and resources in our community and beyond.

V. Shared Governance

In October 2003 the Board of Trustees defined Shared Governance to be:

Within the College's statutory role and mission and the Board of Trustees' operational mission, all constituencies have a role and a responsibility in assisting the College to achieve excellence in all areas of College activity. In pursuing excellence, the Board of Trustees welcomes and expects the participation of faculty, students, staff, and other College constituencies in the decision-making process. The Board of Trustees encourages a broad exchange of information and ideas. To facilitate the exchange of information and ideas, the Board of Trustees looks to the President of the College as its primary liaison with the College constituencies. To be effective in this role, the President must establish an open environment of communication with all members of the College community and establish avenues for consultation and recommendation by faculty, students, and staff regarding policy matters considered by the Board of Trustees. The Board of Trustees delegates to the President, as the chief executive officer of the College, full authority and responsibility for administering the College within the policies and procedures established by the Board of Trustees. Within this delegation is the expectation that the President will elicit the participation and facilitate the fulfillment of the roles and

responsibilities of the College's campus constituencies in the College's internal decision-making processes. It is through the initiative, participation, and effort of all the College's constituencies that excellence is achieved.

VI. Information Technology Governance

"Shared governance" is the process of securing user input on such issues as direction, establishing priorities, reviewing technology decisions, and providing effective user communication in systems development and daily operations. The governance process is meant to involve those individuals, departments, programs, and interests served by the technology resource in meaningful and significant participation.

Metro State's vision of leveraging information technology to enhance the academic mission of the college requires an IT oversight capability, or governance, that ensures equal and proper involvement of all areas of the college infrastructure in IT investment decision making process.

The functions of the Division of Information Technology are somewhat unique when weighed against those of most departments within Metro State. The division was founded to provide technology-based services to all elements of the college within which it operates. Since it is service-oriented, this organization must receive continual feedback from the college community concerning direction and performance.

Because of its technical nature, provision of IT services requires unique control methods that would normally not be applied to any other academic function. These controls must ensure that the best interests of the college are served while at the same time, ensure that the services offered to users are relevant and cost effective. This form of control is best applied through the use of an "IT Governance" structure.

To exercise proper oversight in the planning, acquisition and deployment of IT, a three-tiered governance group has been established. The highest level is the President's Cabinet. Reporting to the Cabinet is the Information Technology Executive Advisory Committee. Reporting to the Committee is a functional committee, the Technology Initiatives Committee. Also, three other functional committees, the Lab Advisory, Banner Managers and Portal Advisory Committees serve to advise both the Executive Advisory and the Initiatives Committees. The functional committees should meet not fewer than three times during the Fall and Spring semesters. Other functional committees may be formed as the college identifies new initiatives, such as Online Education and specific departmental projects.

The college's Chief Information Officer is responsible for the IT environment at Metro State. The CIO Chairs the Executive Advisory Committee that is responsible for IT policy and oversight of the IT environment. The Initiatives Committee is responsible for preparing strategic and policy IT matters to be considered by the Executive Advisory Committee. The other functional committees coordinate their projects with the Initiatives Committee to ensure that an overall college perspective is used when implementing new IT technologies and/or strategies.

Through this Governance structure, along with the Annual Academic and Business Planning processes, Metro State is ensuring maximum educational and business value for its IT investments.

VII. Information Technology Executive Advisory Committee

The Information Technology Executive Advisory Committee (ITEAC) is responsible for information technology policy and with technology change as it affects instructional methods, research, outreach, and administrative processes. It also serves as the committee responsible for matters concerning global initiatives for technology. Activities covered under this structure are related to academic, administrative, lab, and shared college technology resources. The committee's primary purpose is to bring equity and planned focus to the distribution of college information technology resources and not to make equipment decisions relating to specialized departmental requirements. The focus of this committee is priorities, planning, funding, and policy issues. Among the roles that this committee is charged with includes:

- Identify and maintain both short and long range strategic plans for IT.
- Review project and procurement priorities with established plans.
- Review and recommend academic, administrative, and other IT policy issues.
- Ensure that major technology related initiatives are communicated to the campus and funded accordingly.
- Serve as the focal point for input on computing matters and concerns.

Membership

Vice President of Information Technology and Chief Information Officer, Chair
Provost and Vice President of Academic Affairs
Vice President of Student Services
Vice President of Administration and Finance
Vice President of Institutional Advancement
Assistant Vice President of College Communications

Chair of Technology Initiatives Committee
Dean, School of Business
Dean, School of Letters, Arts, and Sciences
Dean, School of Professional Studies
A representative from Student Government
Assistant Vice President of Information Technology

VIII. Technology Initiatives Committee

The primary purpose of this committee is to ensure that technological initiatives serve to enhance or supplement the teaching mission of the college and functions at the ITEAC's direction. The focus of the committee is to determine which new technologies are needed for the college to continually meet its teaching and learning objectives. All matters of policy, strategy, and management of the IT environment should be reviewed by the Initiatives Committee and forward these matters or issues to the ITEAC with their recommendation. The chair of this committee is selected at the start of each academic year by Faculty Senate. One director from IT will work with the committee chair to co-chair the meeting. The committee should meet a minimum of three times during the Fall and Spring semesters. The roles of this committee include:

- Recommend short and long-range strategic plans for shared academic IT resources (not including school, departmental, or student lab plans for special purpose computing requirements).
- Coordinate and review the short and long-range plans for general academic and specialized computing use, including the use of online teaching services.
- Review and recommend service-related policies for academic computing, including online academic computing needs.
- Review and recommend priorities for projects and procurements for academic computing.
- Work in conjunction with the ITEAC in establishing and articulating an evaluation and review process for computing across the College.
- Work with the other functional committees to address the college-wide IT strategy and any initiatives that they bring forth.
- Additional responsibilities as determined by ITEAC.

Membership

Vice President for Information Technology (Ex Officio)
Director, Faculty Resource Center

Chair of Mathematical and Computer Sciences Department or designee and two additional representatives from the School of Letters, Arts, and Sciences
Chair of Computer Information Systems Department or designee and one additional representative from the School of Business
Two representatives from the School of Professional Studies
Director of Server Support Services (Co-Chair)
Director of Network and Desktop Support Services
Information Security Officer (Ex Officio)
One representative appointed by Faculty Senate to serve as Chair
Two student representatives
One representative from Academic Affairs
One representative from Administration and Finance
One representative from Student Services
Chair, Lab Advisory Committee
Chair, Banner Manager
Chair, Portal Advisory Committee

IX. Other Functional Committees

The college has three other committees that are formally concerned with matters relating to IT. The other committees address operational matters that pertain to the Student Lab, Administrative Computing, and Portal/Web environments. These committees are important to the overall success of the college's IT environment and should meet a minimum of three times per Spring and Fall semesters. Additional functional committees, such as the Online Task Force, may be formed to address significant computing issues that may impact the campus. The following is a brief description of the ongoing committees:

Lab Advisory Committee

The primary purpose of this committee is to ensure that Student Lab resources are used to enhance or supplement the teaching and learning mission of the college. The focus of the committee is to develop and recommend policies, potential uses, and software requirements needed to provide students with the technology they need to complete coursework and succeed in their educational pursuits, as well as provide computer classrooms for faculty to use in teaching. The chair of this committee is elected at the start of each academic year. One director from IT will co-chair the committee and help facilitate the meetings. The roles of this committee include:

- Recommend short and long-range strategic plans for student labs (not including school or department labs).
- Coordinate and review the short and long-range plans for general academic and specialized computing use with the Technological Initiatives Committee.

- Review and recommend service-related policies for student computer labs.
- Review and recommend priorities for projects that impact the student labs.
- Additional responsibilities as determined by the ITEAC.

Banner Managers Committee

The primary purpose of this committee is to ensure that Administrative computing resources are used to enhance or supplement the mission of the college. The focus of the committee is to develop and recommend policies, identify issues and recommend solutions for Banner. The chair of this committee is elected at the start of each academic year. One director from IT will co-chair the committee and help facilitate the meetings. The roles of this committee include:

- Recommend short and long-range strategic plans for administrative computing.
- Coordinate and review the short and long-range plans for administrative computing use with the other functional committees and Technology Initiatives Committee.
- Review and recommend Banner related security policies.
- Review and recommend priorities for projects and implementation of Banner upgrades.
- Work to establish and articulate an evaluation and review process for administrative computing projects and administrative policies.
- Additional responsibilities as determined by the ITEAC.

Portal Advisory Committee

The primary purpose of this committee is to ensure that the college's Web and MetroConnect services are used to enhance or supplement the mission of the college. The focus of the committee is to develop and recommend policies, identify issues and recommend solutions for MetroConnect and web related services. The chair of this committee is elected at the start of each academic year. One director from IT will co-chair the committee and help facilitate the meetings. The roles of this committee include:

- Recommend short and long-range strategic plans for portal and web services.
- Coordinate and review the short and long-range plans for the college's portal and web services with the other functional committees.
- Review and recommend priorities for projects and implementation of web and portal upgrades.
- Work to establish and articulate an evaluation and review process for Portal and Web related projects.
- Additional responsibilities as determined by the ITEAC.

XIX. Network Security Policy for Metropolitan State College of Denver

I. Purpose:

To establish policies, procedures and guidelines for securing Metro State College's computing network (both wired and wireless).

II. Scope:

These policies affect all users who use Metro's networking (wired or wireless) resources.

III. Introduction:

Metro's computer network (both wired and wireless) exists to support the college's educational mission and related administrative functions. The network provides access to information and other resources that are important to all of the college's educational and administrative units. Some of these resources are available to the public, while others are available only to members of the Metro State community. Access to information resources containing confidential information about members of the college community is restricted to authorized personnel only. The college has both legal and ethical obligations to safeguard these resources.

The Department of Information Technology (IT) is responsible for developing, implementing, and monitoring the administrative, technical and physical controls necessary to protect the integrity and availability of the college's networking resources, and to protect the confidentiality of the data transmitted over the network or stored on network connected devices. The Network Security Policy is an essential element of a larger administrative framework that guides and governs the development and implementation of these security controls.

IV. Policy Statements:

1. The college network is divided into multiple security zones.
 - a. Networked devices, including workstations and servers, which can be accessed directly from the Internet are placed into a separate security zone specifically for internet facing services. The college's ERP database and other services requiring higher security standards are placed into a high security zone. All other workstations, servers, services, and other network devices are placed into intermediate security zones.
 - b. Connectivity between security zones is carefully controlled and monitored [see #7 below].
 - c. Connectivity from a lower security zone to a higher (or equally rated) security zone is "That which is not explicitly permitted is implicitly denied." (default deny).

- d. Generally, connectivity from a higher security zone to a lower security zone is "That which is not explicitly denied is implicitly permitted." (default permit).
 - e. IT is responsible for managing the connectivity between security zones.
2. IT is responsible for building and maintaining Metro State's computing network (both wired and wireless). Information Technology will work with departments, faculty, students and staff to develop secure, reliable and cost effective solutions for their networking needs.
3. People using the college's network, or any of the college's other computing resources, must comply with the Responsible Use of Information Technology Resources policy and all other related policies. See: <http://www.mscd.edu/~infotech/policies/>
4. Devices connecting to the college's network must comply with IT networking standards and architecture. Persons desiring to connect devices, other than generic computers and printers, to the network must consult with the IT Network Operations Center before connecting the device. (Call: (303) 556-8325).
5. The Metro State network provides Dynamic Host Configuration Protocol (DHCP) services to dynamically assign IP addresses; devices connecting to the network should use the DHCP protocol to obtain a dynamically assigned IP address. Persons with special equipment or software, which supports the college's educational mission, that requires a static IP address may request one from the IT Network Operations Center. (Call: (303) 556-8325).
6. IT uses both proactive and reactive techniques to defend the network from potential security threats and active security exploits.
 - a. Proactive techniques include: Devices connected to the network are subject to automatic device discovery, and may be periodically tested (over the network) for problems which may pose a security threat to the network or the individuals using the device. These tests will not cause harm to either the device or the user. If a potential security problem is discovered, it will be reported to the personnel (when known) who are responsible for the maintenance of the device.
 - b. Reactive techniques include: IT will isolate or disconnect, without prior notice, any device that is threatening the availability or integrity of the network, or threatening the confidentiality of the data transmitted across the network, or is being used to violate the

Responsible Use of Information Technology Resources policy or other related policies. When known, IT will make every effort to notify the personnel responsible for the operation and maintenance of the device as soon as possible of the disconnect.

7. IT will maintain a variety of network monitoring equipment to monitor the health and performance of the network. Other monitoring equipment will include network intrusion and prevention systems placed in strategic locations throughout the network. IT does not routinely monitor the web sites a user visits or record other network traffic; however, when diagnosing network problems or investigating network anomalies, IT may use diagnostic equipment that does record and analyze all data passing across the network. Data gathered in this manner is rarely retained. IT personnel are obligated to protect the confidentiality of the data they have access to. However, extenuating circumstances, such as the discovery of criminal activity, may require IT personnel to disclose their finding to the college's legal counsel and law enforcement personnel.
8. Access to the college's primary networking equipment is restricted to authorized personnel.

V. Reporting Violations:

Any suspected violations of these policies, or unauthorized access to computing resources, or any other condition which could compromise the security of the college's computing resources must be reported to the Department of Information Technology Security and Disaster Recovery Coordinator, <http://www.mscd.edu/~infotech/security/>, (303) 556-8325.

VI. Remedies for Non-Compliance:

Failure to comply with these policies may result in one or more of the following actions: a) suspension of access to the network for the individual, or educational or administrative unit violating the policy, b) when appropriate, disciplinary action ranging from warning to termination and (for students) expulsion from the College, depending on circumstances, in accordance with applicable policies and procedures, c) when appropriate, initiation of civil or criminal proceedings.

VII. Authority:

The Office of the President grants authority to the Vice President of Information Technology to oversee compliance with this policy.

Questions regarding this policy, or requests for variances from the policy, should be directed to the Vice President of Information Technology at (303) 556-2441.

XX. Electronic Survey Policy and Guidelines for Metropolitan State College of Denver

I. Policy Statement

The Metropolitan State College of Denver employs consistent procedures for notification and processing mass electronic surveys to the following constituencies: faculty, staff (academic and non-academic), students, and alumni. The college expects anyone sending electronic surveys to any or all of these constituencies to do so in accordance with the procedures outlined in this document.

Outside vendors and organizations not directly employed by the College must work with and through the proper vice presidential area to survey Metro State students, faculty and staff. For planning purposes; the survey development and implementation process will take a minimum of ten (10) business days.

II. Reason for Policy

Unsolicited e-mail and excessive surveying of the student body is a major concern of the college. The college must exercise appropriate control over electronic surveys so it may properly maintain network performance, limit the number of unsolicited e-mail messages and maintain the effectiveness of the electronic survey mechanism.

III. Exceptions

This policy shall not be construed as limiting faculty members' ability to conduct research. Surveys conducted by faculty which pertain solely to the conduct and administration of the class or classes that they teach are exempt from this policy.

This policy is also not intended to impact or replace existing Student Government election systems and processes.

IV. Definitions

Electronic Survey: A scientific gathering of a sample of data or opinions considered to be representative of a whole, including thorough data analysis to assist in the formal decision making process in an on-line environment. Survey design and analysis of survey data must be confirmed through the Office of Institutional Research.

Electronic Quick Poll: A non-scientific method utilized to obtain a general perception of the population in a short period of time in an on-line environment. The data collected from quick polls should not be treated as scientific or

necessarily factual. Quick poll questions are presented in a completely objective format, i.e. true/false and multiple-choice. Current results of quick polls may be presented on-line in real-time as each participant completes the poll.

V. Justification for an Electronic Survey

Individuals wishing to solicit information from various constituencies on campus through electronic surveys and quick polls are encouraged to review the "Survey Justification Checklist" available in the appendix of this document. This checklist can be used as a tool for survey developers in determining if an electronic survey or quick poll is the best means available to meet a project's goals and objectives.

VI. Policy and Procedure

Surveys

The steps for conducting a formal, on-line survey through the College's systems are as follows, in accordance with the flow diagram in the appendix:

1. After reviewing the Human Subjects Review Policy and Procedures to ensure the survey follows required guidelines or is exempt from the Policy, submit the survey to the Human Subjects Review Committee. The following link describes the Human Subjects Review Policy and Procedures, including submission to it:
<http://clem.mscd.edu/~forrestj/HSRC.htm>
2. Submit the exempted or approved request to the appropriate Vice President or Dean.
3. Receive initial approval of the Vice President over the requestor's division. In the absence of the Vice President over the area, the Assistant Vice President for College Communications must validate and give initial approval of the survey.
4. The individual wishing to conduct the survey and the Vice President will consult with the Assistant Vice President for College Communications as to the substance of the survey. In addition, the administrative officer who approved the survey will inform and seek approval from Cabinet, as appropriate, for the survey request.
5. Upon final approval the responsible administrator or designee will coordinate final development and dissemination of said survey through the Office of Institutional Research. This will insure accuracy, that the survey measures what it is intended to measure and that a valid population selection is utilized.

6. Survey data will be analyzed and distributed in a timely manner through the Office of Institutional Research. Raw data should be made available as well. Data from surveys conducted through outside firms such as Noel Levitz should be made available to the Office of Institutional Research upon request.

The survey itself shall be located and conducted in a standard location within MetroConnect to provide the necessary authentication services while preventing duplication and weighting of data.

Quick Polls

The steps for conducting a quick poll to students, faculty or staff are as follows:

1. After reviewing the Human Subjects Review Policy and Procedures to ensure the quick poll follows required guidelines or is exempt from the Policy, submit the quick poll to the Human Subjects Review Committee. The following link describes the Human Subjects Review Policy and Procedures, including submission to it:

<http://clem.mscd.edu/~forrestj/HSRC.htm>
2. Submit the exempted or approved request to the appropriate Vice President or Dean for that constituency (i.e. students, faculty, and staff).
3. The specific vice president or dean will decide whether it is appropriate for distribution to his or her population.
4. If the specific vice president or dean approves, he or she should consult with the Assistant Vice President for College Communications as to the content of the quick poll.
5. Only the approving vice president or dean may instruct the Metro State Information Technology portal administrators to post/send the quick poll.
6. The Metro State Portal Administrators will make the quick poll available in a test environment and contact the sender for final approval before dissemination. Once approved, the quick poll will be made available in the production environment.

VII. Access Priority

In the event of multiple departments wishing to survey constituents within the same timeframe, the following shall serve as a priority access list from highest to lowest priority:

1. Board of Trustees, the President of the College
2. Administrative Divisions of the College through the appropriate Vice President
3. Student Government through the SGA President
4. Other proposed and approved polls through divisional channels

All requests to survey students, faculty and staff should be reviewed by the Office of Institutional Research to insure validity and determine the best methods, including timeframes, for conducting the poll. OIR will be responsible for tracking surveys and data to prevent duplicate efforts by those wishing to conduct said surveys.

VIII. Results

OIR is responsible for analyzing the data and providing results to the surveying party within 72 hours. Should the survey requestor desire the data in a certain format, they should submit a request to OIR in writing and allow five (5) business days for processing. Special requests, such as contracting with an outside firm, for data analysis should be discussed and coordinated with OIR during the initial development of the survey.

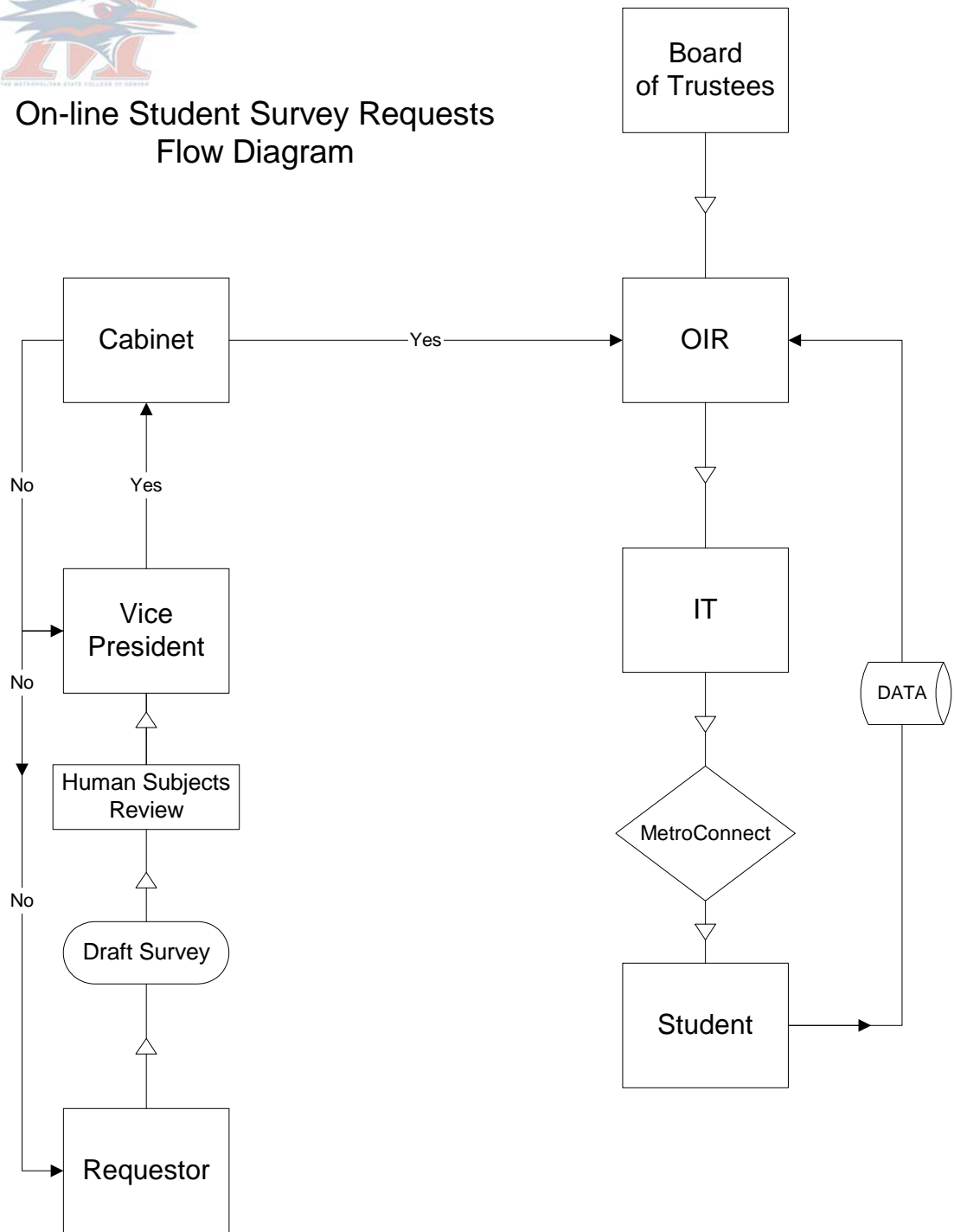
IX. Participation

Those conducting surveys and quick polls at Metro State may not force or compel users to participate in any way. The survey requestor is responsible for initiating all publicity for their respective surveys and polls. Active surveys and polls may be publicized through media tools such as MetroConnect announcements, Today@Metro, Metonline, The Metropolitan, flyers, posters, and any other format the requestor deems appropriate.

Appendix

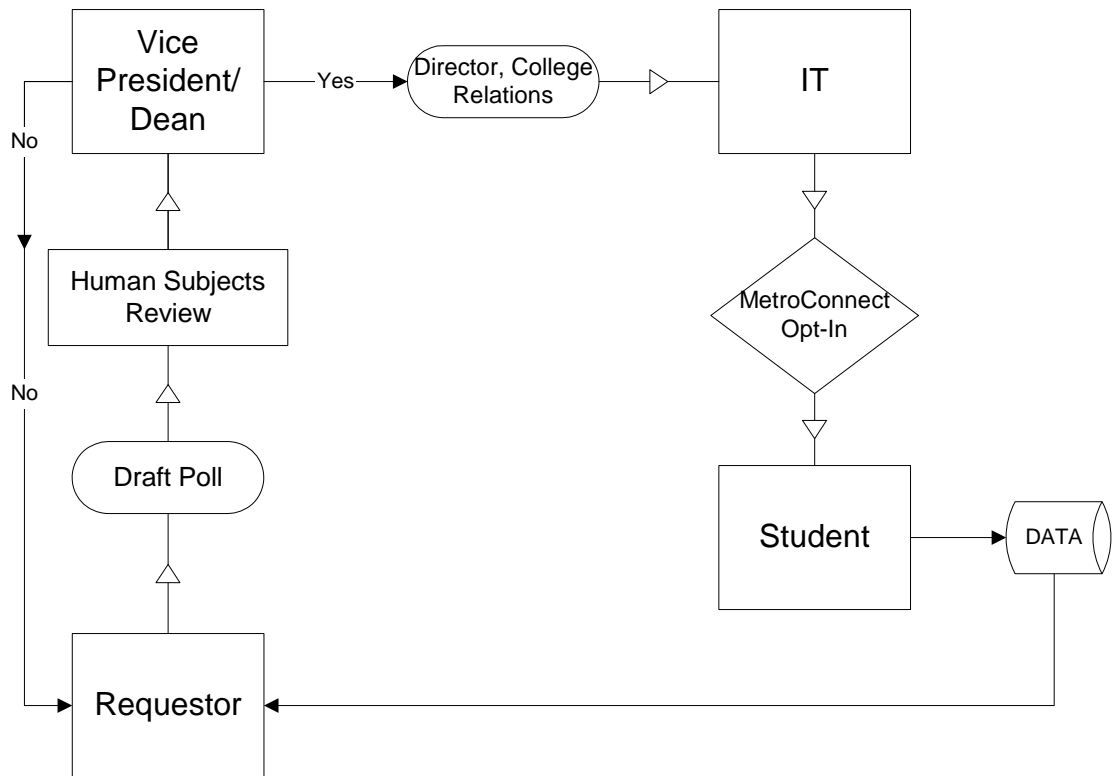


On-line Student Survey Requests Flow Diagram





On-line Student Quick Poll Requests Flow Diagram



Survey Justification Checklist

1. Does the survey/quick poll relate to official college business?
2. Define Goals and Objectives - What you want to learn and Why:
 - Ratings of current products or services
 - Employee attitudes
 - Customer satisfaction levels
 - Reader/viewer/listener opinions
3. How will the results be utilized and disseminated?
4. Is an e-survey or Quick Poll the appropriate/only methodology
 - Face-to-face i.e. focus group or interviews
 - Telephone
 - Mail
 - Web survey vs. e-mail survey
 - Must the data be statistically valid?
5. Determine your sample - Whom you will interview
 - What is your target population
 - Is it possible to identify population using current College data?
 - What is the Sample size? Based on: time available, and necessary degree of precision
6. Do you have the skill/resources to create your questionnaire i.e. what you will ask, how you will ask it.
 - Writing meaningful, valid questionnaires is a skill. A few things to keep consider:
 - Keep it short and simple
 - Introduction or welcome message
 - Allow 'Don't know' or 'Not Applicable' responses where appropriate
 - Question types: Multiple choice, numeric open end, text open end? Rating scales and agreement scales?

Additional resources for developing surveys and survey questions are available at:

<http://www.statpac.com/>

XXI. Password Policy for Metropolitan State College of Denver

I. Purpose

To establish policies and guidelines for the selection and use of passwords used to access Metropolitan State College of Denver's computing resources.

II. Scope

These policies apply to everyone having access to Metropolitan State College of Denver computing resources including, but not limited to, Metro Connect, Email, Windows, Macintosh, and UNIX services, BANNER, remote access, and systems administration and network administration.

III. Summary

Persons accessing password protected computing resources at Metropolitan State College of Denver are required to use strong passwords that are difficult to guess or crack. Passwords must be changed at least once every 120 days.

IV. Introduction

For passwords to be an effective security control, they must be chosen, stored, and managed appropriately. Poorly chosen passwords can be easily guessed or cracked and then used by someone who is not authorized to have access to the computing resource. Likewise, passwords that are inappropriately stored could be discovered and misused by unauthorized persons.

V. Policy Statements

1. On computing systems that use passwords as an authentication mechanism, every computer account must have a non-blank password.
2. All user and system passwords are to comply with the requirements listed in the Requirements section below.
3. Passwords must be changed:
 - a. Immediately upon first logon.
 - b. At least every 120 days. Passwords which have not been changed within 120 days are subject to being systematically expired.
 - c. When there is reason to believe the password has been compromised.
 - d. For accounts with access to administrative computing resources, immediately upon departure of personnel having access to those accounts.

4. Passwords are not be posted on, under, or around a computer or in the work place.
5. Persons using Metro State computing equipment are not to make use of the "Remember my password" or "Automatic login" options that are provided by some application programs and web browsers.
6. Passwords are to be kept secret. Passwords are not to be shared with coworkers, family, friends, IT, or other people. No one in the Department of Information Technology, including the Help Desk, needs to know your password and should never ask you for your password.
7. The use of password guessing, password cracking or keystroke logging software is prohibited without a court order or the written authorization of the College's legal counsel and at least one other member of the Presidents Cabinet. Any such activity is to be fully documented. Any data gathered by such activity is to remain confidential and is to be protected from unauthorized disclosure, use, or modification.

VI. Requirements

1. The following requirements describe the creation of strong passwords:
 - a. A password must be at least eight (8) characters in length. A password may be longer than eight characters.
 - b. A name or a word from the dictionary may not be used as a password.
Two or more unrelated words may be combined.
 - c. A password must contain a mixture of upper and lower case letters, and numbers or punctuation marks. A password must contain:
 1. Two or more upper case letter from the alphabet (A-Z).
 2. Two or more lower case letter from the alphabet (a-z).
 3. Two or more decimal digits (0-9) or punctuation marks, or a decimal digit and a punctuation mark.
 - d. A password must not contain a simple pattern or sequence of numbers or characters, such as "xyz123".
 - e. A password must not contain a persons student id/employee id number, social security number, date of birth, telephone number, or any other information that could be easily guessed or discovered about the individual.

- f. An old password must not be reused for at least 1 year from the date it was changed.
 - g. A new password must have at least three (3) or more characters which differ from the previous password.
2. Passwords used to access Metro State computing resources are not to be used to access non-Metro State computing resources.

VII. Roles and Responsibilities

Everyone who is authorized access to Metro State password protected computing resources is responsible for complying with these policies and guidelines.

Supervisors are responsible for instructing their employees regarding these policies.

System Administrators/Database Administrators will configure their systems to enforce as many of the above password requirements as possible. When a system lacks the ability to enforce one or more of the most significant password requirements, these deficiencies will be documented and communicated to the Security Coordinator.

Computer systems will be configured to log all failed login attempts. The log entry should include the date, time, username attempting to login, and the source IP address from which the login attempt was made.

Computer systems will be configured to disable an account for some indefinite period of time upon 5 successive failed login attempts to the account. A log entry should be recorded anytime an account is so disabled.

VIII. Exceptions

Under rare and specific circumstances, it may be necessary to petition the VP of Information Technology for a waiver of a portion of the password policy. The request for a waiver must be made in writing and must include a compelling business justification for the waiver, document what portion of the policy the waiver is for, who the waiver is for, how long the waiver will last, and how any risks introduced by the waiver will be managed. Granting a waiver of the password policy is not automatic. A petition for a waiver could be denied simply because of technical or security reasons.

IX. Reporting Violations

Any suspected violations of these policies, or unauthorized access to computing resources, or any other condition which could compromise the security of the college's computing resources must be reported to the Department of Information

Technology Security and Disaster Recovery Coordinator,
<http://www.mscd.edu/~infotech/security/>, (303) 556-8325.

X. Remedies for Non-Compliance

Failure to comply with these policies may result in one or more of the following actions: a) suspension of access to the network for the individual, b) when appropriate, disciplinary action ranging from warning to termination and (for students) expulsion from the College, depending on circumstances, in accordance with applicable policies and procedures, c) when appropriate, initiation of civil or criminal proceedings.

XI. Authority

The Office of the President grants authority to the Vice President of Information Technology to oversee compliance with this policy.

Questions regarding this policy, or requests for variances from the policy, should be directed to the Vice President of Information Technology at (303) 556-2441.

XXII. Automatic Timeout of Idle Sessions

I. Purpose

To establish policy for the automatic termination of idle or abandoned interactive computer sessions.

II. Scope

These policies apply to all computing systems at Metropolitan State College of Denver that are operated by the Department of Information Technology including, but not limited to, MetroConnect, BANNER, UNIX, and remote access services.

III. Introduction

Interactive computing sessions established via a Web browser, remote terminal session, telnet, ftp, ssh, sftp, or VPN create a security threat anytime such an interactive session is abandoned by the user. In addition to the security threats created by abandoned interactive computing session, every interactive computing session has a large number of computing resources allocated for it to support the session; these resources remain allocated to the session until the session is terminated. Interactive session which have been abandoned consume computing resources and compete with other interactive sessions that have not been abandoned.

IV. Policy Statements

1. Persons establishing an interactive computing session with an MSCD computing resource are required to log out of the interactive session when they have finished their work and anytime they will be away from the computer for an extended period of time.
2. Information Technology will establish appropriate time-out limits for each interactive computing services as determined by the Vice President of Information Technology. Interactive computing sessions which do not perform some form of input/output during the defined time-out period will automatically be disconnected from the service.
3. All workstations will be equipped with an automatic screen saver that will blank out the screen and lock the workstation after a period of inactivity. The user will be required to re-enter their password to unlock the workstation and un-blank the screen.

V. Authority

The Office of the President grants authority to the Vice President of Information Technology to oversee compliance with this policy.

Questions regarding this policy, or requests for variances from the policy, should be directed to the Vice President of Information Technology at (303) 556-2441.

Approved by the Cabinet, October 23, 2006

Next Review Date: September 2008