EXECUTIVE ORDER NO. 76

EFFECTIVE DATE: **October 10, 2000**

SUBJECT: **METRO NETWORK ACCESS POLICY**

PURPOSE AND SCOPE

Compliance with Metro's network access policy will ensure the integrity and security of Metro's shared information resources. Following these guidelines will help keep all of our work safe.

This policy applies to all network users, including employees, interns, temporary help, volunteers, government officials and any other person who has or will have access to the network. All computers, programs, documents and data generated, processed and/or stored on the network or users' workstations are Metro property by ownership or license agreement. Employees may access only files or programs, whether computerized or not, that they have permission to enter.

For purposes of this policy, the components of the network are:

- All cabling used for carrying voice and electronic information
- All devices used for controlling the flow of voice and electronic information including, but not limited to, switches, hubs, routers and servers
- All computer components including, but not limited to, monitors, cases, storage devices, modems, network cards, memory chips, keyboards, mice, cables, diskettes and other media, laptops and Personal Digital Assistants (PDAs)
- All computer software
- All output devices including printers and fax machines

Metro reserves the right to retrieve and read any document, email message, Internet history log or other electronic media that is composed, sent or received. This includes the right to retrieve or recreate any message or document that was deleted.
The remainder of this document focuses on issues regarding your network access, use of technical resources and security.

PHYSICAL ACCESS

Terminate the network connection if your computer will be left unattended for more than four hours. You can reboot or turn off the computer; the newer Windows operating systems (NT, 98 and 2000) and Macintosh OS 8.5 and newer allow a secure logoff without rebooting the machine.

NETWORK ACCESS

Requests for access to the network, and/or any equipment on the network, including new user setups, access rights changes and terminations, should be made by your supervisor to the Help Desk. The Information Technology (IT) Department will set up appropriate access within three business days. Each user will have a unique user ID and password. Never sign on as another person or attempt to access systems in an unauthorized manner. Contact the Help Desk if you would like a review of your access.

PASSWORDS AND USER IDS

Passwords and user IDs are critical for computer security. Use only your assigned user ID. You are accountable for the content of all text, audio or images that you place or send over Metro's technical resources, or that is placed or sent using your user ID. Carefully select a password for use with your user ID. Every user ID will have a password. Passwords are to be at least six (6) characters long, changed at least every 30 days, unique (different than the last 10 passwords), and kept private at all times.

Although you may have passwords to access computer, voicemail and e-mail systems, these technical resources belong to Metro, are to be accessible at all times by Metro and are subject to inspections by Metro with or without notice. Metro may override any applicable passwords or codes to inspect, investigate or search users' files and messages without any prior notice to the user(s).

You should not provide a password to other users or to anyone outside Metro and you should never access any technical resources using another employee's password. Unique circumstances exist where collaboration is necessary. These situations are to be reviewed by the I.T. Director to ensure appropriate controls exist. Use without that express approval is considered an infraction of this policy.

Good techniques for creating a password are:

- Two short words connected by punctuation (dog/rain, book+mug);
- The first letter of a series of words in a poem ("Mary had a little lamb whose fleece was white as snow"...mhallwfwwas)
- Pronounceable nonsense words made alternating one consonant between one or two vowels, such as "quadpop" and "routboo"

Poor choices are family names, personal numbers others can obtain (social security, license plate, telephone, address, etc.), pet's names, etc.

HARDWARE

The I.T. Department coordinates adding, removing, moving or changing any network equipment (*see page 1 for the definition of network equipment).* Call the Help Desk to request assistance. The Help Desk will have a schedule for you within three business days. Do not connect or disconnect anything without approval from the I.T. Department.

SOFTWARE

The I.T. Department coordinates all software installation on computers and the network. Since software products can cause conflicts with other software in computers, the I.T. Department manages certain products to avoid difficulties. However, in special cases, the user may require special software. Users may install special use software after consultation and approval of the I.T. Department and the user's director or supervisor. All data on the network is governed by Metro's document retention policies. These policies must be used in conjunction with any decisions made by users about the retention of data. Record retention is a complex issue, and users are advised to thoroughly understand retention requirements related to their area. Your department records coordinator will have the information for your department.

VIRUS PROTECTION

Virus protection software runs on workstations and on the network. Never disable any virus protection software. Any evidence of or notification of a virus should be reported to the Help Desk immediately. All computer media (floppy disks, high capacity zip disks, CD's, tapes, etc.) that has been used in a non-Metro computer must be scanned for viruses before use in a Metro computer. When in doubt, contact the Help Desk before using the non-Metro disk.

E-MAIL AND INTERNET USE

E-mail is a network-based electronic communications tool to be used for Metro business. In-coming and out-going e-mail is not scanned for viruses. Users need to observe the virus protection procedures above, especially before opening electronic attachments and downloaded files.

Access to the Internet is provided as a tool for users to conduct Metro business, in accordance with Metro's Internet Usage Directive. The use of the Internet is for Metro business only. Managers may permit limited personal use of computers and the Internet when it is less disruptive to permit employees to do so than to require an employee to take a break or leave work to take care of personal matters.

Personal use of computers during working hours requires the permission of your manager. Managers can restrict use as it relates to personal use. If approved, such use must be brief, infrequent and otherwise comply with all Metro rules and policies. Any personal use should not interfere with Metro business or individual job performance. Personal reliance on workplace computers and Internet access in order to avoid the financial expense of obtaining personal equipment or services is a violation of state law.

Prohibited uses include, but are not limited to:

- Hacking, or illegally attempting to access any network equipment owned by Metro or any one else
- Communicating with pen pals
- Personal gain and/or financial benefit
- Accessing pornographic or hate sites
- Junk mail, SPAM, chain letters or unsolicited announcements
- Personal or social announcements not work related.
- Disobeying copyright laws and software licenses
- Sharing confidential materials, comments or any password, identifying code, personal identifying number or other confidential information without the permission of its' owner. This includes your Metro password(s).
- Any political communication that violates Oregon or federal law.

Metro's technical resources may not be used for personal gain or the advancement of individual views. Employees who wish to express personal opinions on the Internet must obtain a personal account with a commercial Internet service provider and must access the Internet without using public resources.

Solicitation for any personal business activities using Metro resources is strictly prohibited. Your use of Metro technical resources must not interfere with your productivity, any other employee or the operation of Metro's technical resources.

Email messages may not contain content that may be reasonably considered offensive or disruptive. Offensive content includes, but is not limited to:

- Angry, hostile or threatening material.
- Obscene, indecent, lewd or lascivious material. This includes material that explicitly or implicitly refers to sexual conduct, or contains sexual comments or images.
- Material or comments that would offend someone on the basis of his or her gender, age, sexual orientation, religious or political beliefs, that contains profane, sexist, racist or other discriminatory language, national origin, disability or any other protected class

As an employee, you represent Metro in your communications and actions; it's important you understand how behaviors reflect on the organization.

REMOTE ACCESS

Remote access is the connection of a personal computer at an outside location to Metro's local area network. Some platforms do not currently have this capability. Employees who want to telecommute must have agreement from their supervisor and must sign the "Telecommuting Agreement" as provided for in Executive Order 52. Some government partners have access to parts of Metro's network. The I.T. Department will create access upon approval of the manager or director who is responsible for the requested data.

COMPLIANCE

Everyone has a serious responsibility to keep his/her workstation and the network secure. Violations of any guidelines in this policy may result in disciplinary action up to and including termination. In addition, Metro may advise appropriate legal officials of any violations and cooperate in investigations conducted by legal officials.

SUMMARY

Network security is vital to Metro's mission. Unauthorized access, improper use, or other policy violations should be reported to the Information Technology Department. Notify the IT Help Desk if you believe there is a security problem on the network. Do not demonstrate the problem to other users. If you have any questions, please contact the I.T. Department.

From time to time the Executive Office may supplement this Executive Order with further principles and examples.

Ordered by the Executive Officer this 10th day of October 2000

Mike Burton, Executive Officer

600 NORTHEAST GRAND AVENUE | PORTLAND, OREGON 97232 2736
TEL 503 797 1700 | FAX 503 797 1797

METRO

TO: All Department Directors

FROM: Cathy Kirchner Cathy

DATE: October 10, 2000

RE: Executive Order 76

Attached is a copy of Executive Order 76, Network Access Policy. Please be certain to share this information with your staff.

cc: Jeff Stone, Council Chief of Staff
Alexis Dow, Auditor