



OSHA INSTRUCTION

U.S. DEPARTMENT OF LABOR

Occupational Safety and Health Administration

DIRECTIVE NUMBER:

ADM 1-0.19

EFFECTIVE DATE:

September 8, 2000

SUBJECT: OSHANET Acceptable Usage Policy

ABSTRACT

Purpose: This policy describes and sets forth guidelines for use of OSHANET and any of its resources.

Scope: This instruction applies OSHA-wide.

References: DLMS 9 Chapter 12, Information Technology: Microcomputer and LAN Management; Patricia W. Lattimore Memorandum for All DOL Employees, Reminder on Appropriate Use of DOL Information Technology, May 19, 1997; 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch; and ADM 12-0.4A, Revised OSHA Records Management Program.

State Plan Impact: State Plans on the OSHANET only.

Action Offices: National and Area Offices; 18(b) States and Consultation Projects on the OSHANET.

Originating Office: Directorate of Information Technology

Contact: Directorate of Information Technology
(202-693-1818)
N3661, FPB
200 Constitution Avenue, N.W.
Washington, D.C. 20210

By and Under the Authority of
Charles N. Jeffress,

Assistant Secretary

Cover Page

TABLE OF CONTENTS

ABSTRACT	Cover Page
I. <u>Purpose</u>	1
II. <u>Scope</u>	1
III. <u>Reference</u>	1
IV. <u>Action Information</u>	1
A. <u>Responsible Office</u>	1
B. <u>Action Offices</u>	1
C. <u>Information Offices</u>	1
V. <u>Federal Program Change</u>	1
VI. <u>Definitions</u>	1
VII. <u>Background</u>	1
VIII. <u>Notice of Auditing/Monitoring</u>	2
IX. <u>General Guidelines for Use of the OSHANET</u>	2
X. <u>Personal Use</u>	3
A. <u>Acceptable Personal Use</u>	3
B. <u>Non-Acceptable Personal Use</u>	4
XI. <u>OSHANET Access and Security</u>	5
A. <u>Account Establishment</u>	5
B. <u>Account Modification or Termination</u>	5
C. <u>Passwords</u>	5
D. <u>Logging Out</u>	6
E. <u>Workstation Security for Windows 95/98</u>	6
F. <u>Avoidance of Computer Viruses</u>	6
G. <u>Software Programs</u>	7
XII. <u>Monitoring and Administration</u>	7
A. <u>Network Home Directory (P:\ drive) Storage Space</u>	7
B. <u>Internet</u>	8
C. <u>E-Mail</u>	8

D.	<u>Data Backups</u>	9
E.	<u>Ownership of Software and Data</u>	9
XIII.	<u>E-Mail Usage.</u>	9
A.	<u>Mailbox Management</u>	9
B.	<u>Mass Mailings</u>	10
C.	<u>E-mail Auto-Forwarding</u>	10
XIV.	<u>Internet/Online Services</u>	10
A.	<u>Software Uploading</u>	10
B.	<u>Software Downloading</u>	10
C.	<u>Prohibited Sites</u>	11
XV.	<u>Penalties</u>	11
APPENDIX A - TERMS		A-1
APPENDIX B - STANDARD FORM FOR OSHANET REQUEST		B-1
APPENDIX C - COMPUTER TIPS		C-1
Index		Index-1

OSHANET ACCEPTABLE USAGE POLICY

- I. **Purpose.** This policy describes and sets forth guidelines for use of OSHANET and any of its resources.
- II. **Scope.** This policy applies to all headquarters and field offices of the Occupational Safety and Health Administration (OSHA).
- III. **Reference.**
 - A. DLMS 9 Chapter 12, Information Technology: Microcomputer and LAN Management.
 - B. Patricia W. Lattimore Memorandum for All DOL Employees, Reminder on Appropriate Use of DOL Information Technology, May 19, 1997.
 - C. 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
 - D. ADM 12-0.4A, Revised OSHA Records Management Program.
- IV. **Action Information**
 - A. **Responsible Office.** Directorate of Information Technology (DIT), Office of Management Data Systems (OMDS)
 - B. **Action Offices.** National and Area Offices; 18(b) States and Consultation Projects on the OSHANET.
 - C. **Information Offices.** Regional Offices; OASAM, Information Technology Center (ITC).
- V. **Federal Program Change.**

This instruction describes a Federal Program Change for which State adoption is not required.

NOTE: Although adoption of this instruction is not required, State plans and consultation projects, especially those on the OSHANET, are expected to have similar guidelines in place, particularly as they relate to computer and Internet access and security.
- VI. **Definitions.** See Appendix A for a list of terms and definitions.
- VII. **Background.**
 - A. The Occupational Safety and Health Administration's (OSHA) nationwide network, the OSHANET, provides employees with information technology (IT)resources to help them effectively perform their OSHA duties and

responsibilities. These resources are primarily Government assets, which must be protected from unauthorized modification, destruction, disruption, or disclosure, whether accidental or intentional.

- B. The OSHANET encompasses user workstations, servers, network devices, software, and data communications equipment. OSHANET provides storage for and access to data, access to the Internet, electronic mail (e-mail), and applications. These resources enable employees to use software programs, communicate efficiently with other people, and to access information from diverse sources around the world and specific to the organization. OSHA's Directorate of Information Technology is responsible for the management and administration of the OSHANET.

VIII. Notice of Auditing/Monitoring.

- A. Users are advised that they should have no expectation of privacy while using any Government-owned or leased information technology resources including, but not limited to: information systems; networks; and related hardware and software, such as workstations, servers, word processors, e-mail, spreadsheets, Internet browsers, etc.
- B. Activity using OSHA information technology resources is subject to Freedom of Information Act (FOIA) requests, to monitoring in the course of system administration, and to audit or law enforcement reviews to protect resources from inappropriate use. Documents (including e-mail) maintained on Government computers can be used by parties in litigation against the Government and can be used as evidence on behalf of the Government. Unauthorized use of these resources is a violation of Federal law and can be punished with fines or imprisonment (P. L. 99-474). Anyone using OSHA information technology resources expressly consents to such monitoring, and violations may be reported to the proper authorities.

IX. General Guidelines for Use of the OSHANET. Users shall exercise responsibility in the use of OSHANET resources and adhere to the following guidelines:

- A. Abide by all Federal laws and regulations, including statutes and regulations governing copyrights, software licensing rules, property rights, and privacy rights.
- B. Abide by all Department of Labor and OSHA policies and regulations regarding the use of information technology resources:
 - 1. DLMS 9 - Information Technology; Chapter 12 - Microcomputer and LAN Management

2. Patricia W. Lattimore Memorandum for All DOL Employees, Reminder on Appropriate Use of DOL Information Technology, May 19, 1997.
- C. Accurately represent OSHA and the Government in all communications. Do not misrepresent yourself, OSHA, or the Government or represent a personal view as a view held by OSHA or the Government. For example, if any personal e-mail message could be perceived as OSHA business or opinion, it should include the disclaimer: "The opinions expressed here are my own and do not necessarily represent those of the Government, OSHA or others."
 - D. Make clear in all Internet communications whether the content is recommended, for which action is optional, or is an authoritative interpretation, for which action is mandated. Where new interpretations are involved, recommendations and authoritative guidance require the same clearance as is required for other written communication, e.g., letters and memoranda.
 - E. Do not make statements or send messages that would cause OSHA embarrassment. For example, using your Government e-mail address (.gov) for posting to a non-business-related message board or user group may raise the public's concerns about Government workers, even if the posting occurred during lunch or after normal working hours.
 - F. Do not use offensive, libelous, slandering or harassing language related to another person on the basis of his or her age, race, color, gender, religion, handicap, national origin, sexual orientation or political beliefs.
 - G. Do not access, display, send or copy lewd, pornographic, obscene or sexually explicit language or materials.
 - H. Do not disclose confidential or sensitive information without proper authorization.
- X. Personal Use.** Government-owned information technology resources such as computers and software are provided to accomplish the work of the Agency. OSHA recognizes, however, that some personal use of these resources can be reasonable and acceptable. Users shall apply the following guidelines when using OSHANET resources for personal use:
- A. Acceptable Personal Use. Reasonable personal use of OSHANET resources on a limited basis is permissible under the following provisions:
 1. Use fully complies with OSHANET Acceptable Usage Policy;
 2. Use is consistent with the ethics and conduct requirements for Department of Labor employees set forth at 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

3. Use does not interfere with the conduct of official OSHA business;
4. Use occurs during employee's personal time;
5. Use does not interfere with employee's work;
6. Use does not incur any additional, unapproved direct charges, such as online services that charge on a time or usage basis; and
7. Supervisory approval is obtained for desired activity.

B. Non-Acceptable Personal Use. OSHANET users are prohibited from the following uses of the OSHANET or its resources, unless explicitly authorized by their supervisors:

1. Engaging in political activities that are forbidden by Federal laws such as the Hatch Act;
2. Accessing material that would not be suitable for public distribution in the workplace, such as obscene materials;
3. Using commercial subscription services or electronic discussion groups (e.g., listservs, news groups) that are not related to OSHA business and could result in mailings to an OSHA e-mail address;
4. Playing games or gambling, or becoming involved in chain letters, auctions, or pyramid schemes;
5. Using Internet access for data or discussions that would cause OSHA embarrassment;
6. Engaging in private, for profit business activity or performing computing services for commercial services;
7. Soliciting money for religious, political or personal causes;
8. Possessing, installing, or using programs capable of fraudulently simulating system responses (example: No engaging in hacking, breaking security, or circumventing security controls);
9. Possessing, installing, or using programs (e.g., viruses, worms, Trojan horse, or trap-door program code) that erase or alter files maliciously or without authorization;
10. Interfering with system efficiency or attempting to modify or crash systems;

11. Loading unauthorized or personal software;
12. Modifying or possessing systems control information, especially that which affects any aspect of the system, maliciously or without authorization; and
13. Using another person's user name and password, or attempting to access unauthorized files, directories, or other resources.

XI. OSHANET Access and Security. All users must practice the following basic safeguards to ensure the confidentiality, integrity, and availability of OSHANET resources.

- A. Account Establishment. Requests for new OSHANET accounts must be documented on the *OSHANET Account Action Request* form (*Appendix B*). For the National Office, supervisors must ensure that the form is completed and provided to the Help Desk. For the field sites, the supervisors must ensure that the form is completed and provided to the local OSHANET Administrator.
- B. Account Modification or Termination. For the OSHANET users leaving OSHA or moving from one site to another within the OSHANET, the Help Desk (for the National Office users) or the local OSHANET Administrator (for the field site users) must be notified at least 7 days in advance of any need to modify, move, or delete their OSHANET user accounts. The account will be closed after the employee's last day. However, immediate account termination can be made based on a supervisor's request.
- C. Passwords. Users are responsible for all activities in their OSHANET accounts. Thus, it is important to protect your OSHANET password from disclosure. The security of OSHANET systems and the integrity of the resources it provides depend on many factors. Passwords that are easily guessed or revealed by sharing or writing down can compromise the entire network. The user must adhere to the following constraints:
 1. Passwords must have at least 8 alphanumeric characters. Use non-dictionary passwords (i.e., passwords that cannot be found in a dictionary). Do not use words such as names, places, or things – especially those that can be associated with you.
 2. Passwords will expire after 90 days and must be changed.
 3. Do not write down your password.
 4. Do not store your password in files on the system, such as batch files or startup scripts.
 5. Do not include your password as part of an e-mail message.

6. Do not use your OSHANET password for any other purpose, such as a password for a specific application or another operating system.
 7. Do not let anyone else use your user name and password. (For security reasons, supervisors must not keep lists of subordinates' passwords. If a supervisor requires access to a subordinate's network account, the supervisor must contact the local OSHANET Administrator [for the field site users] or the Help Desk.)
 8. Users need not reveal their passwords to network technicians who are responding to trouble calls. If a user is present, he/she can logon as himself/herself and let the network technician troubleshoot the workstation problems. If a user is not present when a network technician responds to a trouble call, the network technician can logon as himself/herself and troubleshoot the workstation problems.
- D. Logging Out. Passwords are useless as a security feature unless the workstation is returned to the login prompt. Logout at the end of each day.
- E. Workstation Security for Windows 95/98. The Windows NT workstation users, while still logged onto the network, can lock their workstations when leaving workstations momentarily. Windows 95/98 operating systems don't have such a security feature, instead, they offer two options. The Windows 95/98 users either should log off from the network connection and log back on when they return, or should use a screen saver password when leaving workstations unattended. (See Appendix C, VI (Windows 95/98 Password protection))
- F. Avoidance of Computer Viruses.
1. All PC and laptop users face a potential threat from computer viruses. There are two types of viruses: benign and malicious. A benign virus may simply flash an annoying message on the screen, while a malicious virus will destroy information. Viruses are most frequently spread via downloading files from a poorly run bulletin board or File Transfer Protocol (FTP) site, through the use of an infected floppy disk, or from opening an infected e-mail attachment.
 2. Anti-virus software is part of the standard OSHANET workstation configuration. It must be running in the background on your desktop or laptop computer. If you are unsure of the operation of the anti-virus software, please contact the Help Desk.
 3. To minimize virus infection:
 - Scan diskettes for viruses.

- Use caution when accessing files downloaded from bulletin boards, FTP sites or the Internet.
 - Do not open e-mail attachments from unknown or unreliable sources or if you see a caution message about possible viruses.
 - Always save and scan e-mail attachments before opening.
4. If your anti-virus software detects a virus and you are unsure how to proceed, STOP and contact the Help Desk immediately. The Help Desk will assist you in the removal of the virus before it spreads to other parts of OSHANET.
 5. Users should forward any e-mail messages received warning of viruses to their local OSHANET administrators and to the Help Desk for verification and action, as necessary. Users should not forward these messages to other users on their own. It is not uncommon for such warnings to be hoaxes. Only your OSHANET administrators can determine and execute the appropriate OSHANET-wide response.
- G. Software Programs. The security and functionality of OSHANET servers, workstations, operating systems, and standard software configuration must be preserved in order to guarantee appropriate access to all OSHANET resources and services. Only DIT/OMDS-provided software upgrades, patches, service packs, and other updates made available from network drives or other DIT/OMDS authorized distribution methods may be applied to operating systems or software programs that comprise the standard OSHANET software configuration. This standard OSHANET software configuration is published on the OSHA Intranet Web site.

No software product or program that is not properly licensed for use by OSHA may be installed or run on any OSHANET workstation or server. Further, DIT/OMDS may require the removal of any non-standard software product or program installed on an OSHANET server or workstation, if it is determined that the product or program interferes with the operation or security of any OSHANET resources or services.

XII. Monitoring and Administration. Unnecessary, careless, and unauthorized usage can cause network and server congestion, slow network and applications performance, fill-up network disk storage space, and occupy printers and other shared resources. A user's failure to follow appropriate usage and security practices may result in certain restrictions being placed upon that user's account.

- A. Network Home Directory (P:\ drive) Storage Space. All users in the National Office and OSHANET field sites will have a limit placed on their Home directory (P:\ drive) storage space. The storage limit for the field site users' P:\ drive will be established by the local OSHANET administrator and will be consistent with local

server's disk space availability. DIT/OMDS will assist field sites with establishment and implementation of storage space limits on users' Home Directories (P:\ drive). To avoid running out of disk space, periodically (once a week is recommended) review your files and delete the ones you no longer need. (Note: Deletion of files should comply with record retention policies and guidelines issued by OSHA and your organization. Reference: ADM 12-0.4A, Revised OSHA Records Management Program)

Each field site must establish a process to address requests for a higher limit on P:\drive storage space for individual users with a valid need.

B. Internet.

1. OSHANET administrators may block access from within the OSHANET to any known inappropriate or sexually explicit site. If network monitoring of Internet usage indicates that objectionable sites have been accessed, those sites may be blocked for all users.
2. If a pattern of misuse is observed from a specific computer or user account, access to the entire Internet may be blocked for that computer or account.

C. E-Mail.

1. All users in the National Office and OSHANET field sites will have a limit placed on their mailbox storage space. The limit on field site users' mailboxes will be established by the local OSHANET administrator and will be consistent with local server disk availability. DIT/OMDS will assist field sites with establishment and implementation of mailbox storage space limits. Users who exceed 80 percent of the pre-set limit of mailbox storage space will receive an e-mail message requesting them to remove unneeded messages before the local pre-set limit is reached. (Refer to Appendix C: III.a., to find out how to check your mailbox size.) Users that reach the local pre-set limit will not be able to send or receive new messages. Each field site must establish a process to address requests for a higher limit on mailbox storage space for individual users with a valid need. (Note: E-mail messages and attachments may be records. Deletion of files should comply with record retention policies and guidelines issued by OSHA and your organization. Reference: ADM 12-0.4A, Revised OSHA Records Management Program)
2. To prevent very large e-mail messages from slowing the network, the size of Internet e-mail attachments is limited to 10 megabytes for both inbound and outbound e-mail attachments. Messages with larger attachments (more than 10 MB) will not reach their destination.

- D. Data Backups. If the network or your computer crashes or security is compromised, backups can be used to restore the system to a previous state. Files stored in your Home directory on the network P: drive are included in scheduled incremental (daily) and full (weekly) system backups. Therefore, it is recommended that you copy important data files (not the program files/applications) from your local hard drive to your Home directory on the network P:\ drive. However, you should stay within your storage space limit of 50 MB, and should never attempt to copy the entire C:\ drive over to the P:\ drive.
- E. Ownership of Software and Data. All software programs and data stored anywhere on OSHANET and its computers are, and remain at all times, the property of OSHA. Note that even files and messages that have been deleted can sometimes be restored or recreated in the future.

The Government retains ownership to any material posted to any Internet forum, news group, chat room, or World Wide Web page by any employee in the course of his or her duties.

XIII. E-Mail Usage.

- A. Mailbox Management. Managing your mailbox includes organizing important messages so you find information when you need it and permanently getting rid of unnecessary messages so they do not consume storage space on the server. (Note: E-mail messages and attachments may be records. Deletion of files should comply with record retention policies and guidelines issued by OSHA and your organization. Reference ADM 12-0.4A, Revised OSHA Records Management Program)

Responsible mailbox management includes, but is not limited to, the following practices:

1. Avoiding multiple copies of messages. Do not “cc:” yourself when sending messages. A copy of every message you send is automatically placed in the Sent Items folder. Therefore, Sent Items serve the same purpose as a “cc:” to yourself. When replying to a message, you can delete the original message since it is automatically included in the reply.
2. At least once per week, review your Sent Items folder and delete unnecessary messages. Please note that when you delete a message you are only moving it to a folder called Deleted Items. It is still occupying space in your mailbox. To permanently remove a message, you have to delete it from the Deleted Items folder, at which time you will be asked to confirm that you want to permanently delete the item.

3. Do not use your Deleted Items folder as a filing system. If you need to refer to old messages, save them to other folders. Empty your Deleted Items folder at least once a day. (See Appendix C, III. Mailbox Management)
4. Save large message attachments as files, and delete the attachment from the message.
5. Consider incorporating text in the body of a message rather than using attachments.

B. Mass Mailings. The use of OSHANET e-mail to send non-business-related information such as commercial advertising, chain letters, or other unsolicited messages is explicitly prohibited. Sending this type of information to one or more distribution lists or news groups is considered “spamming”, and is a serious violation of this Directive.

C. E-mail Auto-Forwarding. E-mail messages automatically forwarded to another mailbox can, if they are not accepted at the destination mailbox, cause messages to be sent “endlessly” back and forth. This clogs up the network, slows e-mail and other network services for everyone, and may eventually crash the e-mail system and impact other services. Two common causes of this problem are an invalid forwarding e-mail address and a full mailbox. It is important that if you plan to auto-forward your e-mail to another location, make sure you provide the valid and correct forwarding address.

XIV. Internet/Online Services. OSHA encourages its employees to use the Internet to accomplish job duties and further mission goals. Excessive use is prohibited. (Please refer to the Paragraph X.A. *Acceptable Personal Use.*)

A. Software Uploading. No software licensed to the Government may be uploaded or sent to other sites without explicit authorization from DIT/OMDS.

B. Software Downloading.

1. Users may not download and install any software upgrade, patch, service pack, or other update to any operating system and software program included in the standard OSHANET software configuration without prior DIT/OMDS approval. No software product or program that is not properly licensed for use by OSHA may be downloaded, installed, or run on any OSHANET workstation or server.
2. Any file that is downloaded must be scanned for viruses before it is run or accessed.

3. Indiscriminate downloading of files to the network P: drive can quickly consume drive space, degrade application performance, prevent other users from saving their work, and cause a loss of data. Downloading numerous or large files to network drives is prohibited without prior DIT/OMDS approval, coordinated through the local OSHANET Administrator or ADP Coordinator.
 4. Communications-intensive operations such as large file transfer and video and audio streaming and downloading represent significant data traffic that can cause network congestion. These operations should, if possible, be performed only during off-peak times. Video and audio streaming and downloading without an explicit business-related use are prohibited.
- C. Prohibited Sites. If a user finds himself/herself inadvertently connected to a site that contains sexually explicit, offensive or other inappropriate material, the user must disconnect from that site immediately.

XV. Penalties. Unauthorized use of these resources is a violation of Federal law and can be punished with fines or imprisonment (P. L. 99-474). Anyone using OSHA information technology resources expressly consents to monitoring, and violations may be reported to the proper authorities.

APPENDIX A - TERMS

Definitions of several computer and Internet-related terms used in this directive are provided below.

File Upload - To transfer files from a local computer to a remote computer, usually at a networked Web site or File Transfer Protocol site.

File Download - To transfer files from a remote computer, usually at a networked Web site or FTP site, to a local computer.

Hacking - Gaining unauthorized access to computer systems for the purpose of stealing and corrupting data.

Network Home Directory - One of the network directories, named after a user's login name (e.g., *JSmith*), and located in one of the network drives (e.g., *P:* drive).

News groups - A special interest forum where Internet users gather to discuss a wide range of topics, by posting messages and replying to messages from other users.

Off-Peak Hours - The hours before 7:00 a.m. and after 5:00 p.m. Eastern Standard Time (EST).

Spamming - E-mail advertising (electronic junk mail) sent to a large number of recipients. In addition to wasting people's time with unwanted e-mail, spamming also eats up a lot of network bandwidth.

Trojan Horse - A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves, but they can be just as destructive. They contain hidden instructions to destroy files, programs, or File Allocation Tables (FATs). The instructions may be "time bombs," which are triggered by certain dates, times, or user commands.

User Name - A unique alphanumeric character combination that is assigned to a user's account. Also known as a user ID or login ID.

Virus - A virus is a program or a piece of computer code that is loaded onto your computer without your knowledge and runs against your wishes. Most viruses can also replicate themselves. They are dangerous because they will quickly use all available memory and bring the system to a halt. The most dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. The virus is designed to hide inside other programs. The virus travels with these programs, and it is invoked whenever the program is invoked, and it can then infect other programs or files.

Worm - A worm is a special type of virus that can replicate itself and use memory but can not attach itself to other programs

APPENDIX B - STANDARD FORM FOR OSHANET REQUEST

OSHANET Account Action Request

OSHA

U.S. Department of Labor

Account Action Requested: Add Delete Modify Move
Date Action Required By _____

USER INFORMATION

Indicate: Govt. Employee Contractor

User Name: _____
Last Name First Name M.I.

User ID (for existing account only): _____

Directorate/Office: _____

Site Location: _____ Room: _____

Phone: _____

Mail Distribution List Memberships Requested: (Please list)

Other Requests:

(Use this Section for Move Only)

Transfer work files/e-mail to another person on the OSHANET? Yes No

** (If there is no entry for this question, Files/E-mail will automatically be deleted.) **

If yes, to whom? _____

Move From: (Site/Location) _____ To _____

AUTHORIZATION:

POC for Request: Name _____ Phone _____

Signature _____ Date _____

Supervisor: Name _____ Phone _____

Signature _____ Date _____

SYSTEM ADMINISTRATOR ACTION:

Received by: _____ Date _____

Completed by: _____ Date _____

Note: Upon completion, please return to OMDS Help Desk - N3509 (202) 693-2424 at the National Office, or to the local OSHANET System Administrator at the field site.

APPENDIX C - COMPUTER TIPS

I. Personal Disk Storage Space Management

How to check how much storage space we have used?

- A. Checking the Drive Space: It is important to check the drive space on your *Network Home directory (P:\ drive)* on a regular basis, because each user has a limit on file/folder storage on the network.
 1. Drive Space on Local Hard Disk (C:\):
 - a Double Click on **My Computer**.
 - b Right click on **C:** drive, and click on **Properties**. (*C:\ Properties* window appears.)
 - c Under the **General** tab, *Used Space, Free Space, and Total Capacity of C:* drive is listed, along with a **Pie-Chart**.
 2. Drive Space on Your Network Home Directory (P:\)
 - a Click on **Start**, select **Programs**, and select **Windows Explorer**.
 - b Select and highlight your Home Directory on **P:** drive (e.g. *JSmith on P:*). (Contents of **P:** drive are listed to the right)
 - c Click on the **Edit** menu, and click **Select All**. (All the elements of **P:** drive are selected/highlighted.)
 - d Click on the file menu, and select **Properties**. (*Folder Properties* window appears.)
 - e Under the **General** tab, the size of your files/folders storage on **P:** drive, and the total number of files and folders, are listed.

II. File Management

How to safely delete unwanted files/folders?

- A. Delete Old Files to Make More Room: Even with large hard disks available today, you may be running out of disk space. You may eventually need to remove the old files, those that are no longer or rarely used, from your hard disk to make room for new ones. You'll find two general types of files on a computer: *Program files* and *Data files*.
 1. *Program files* are the files that came with the programs installed on your computer. If you are no longer using a certain program, you should consider removing its files as follows:
 - a Click on **Start**, point to **Settings**, and then click on **Control Panel**.
 - b Double click on **Add/Remove Programs**. (*Add/Remove Program Properties* window appears.)

- c At the bottom of the *Add/Remove Program Properties* window is a list of all the programs that you can remove from your system.
 - d Click and highlight the program that you want to remove, and click on the **Add/Remove** button.
 - e Follow the on-screen instructions to complete the task for whatever program you're removing.
2. *Data files* are the files you create by using the programs on your computer. You might also have the data files on your system that you didn't create, but that you downloaded from the Internet. These files might include graphics, sound files, documents, and the like. Files you download can add up quickly. You should be in the habit of removing unnecessary data files from time to time as follows:

- a Click on **Start**, select **Programs**, and then select **Windows Explorer**.
- b Click on the directory that contains the files that you want to delete. The contents of the selected directory appear.
- c In the file list, locate the file that you want to delete and click it. (To select several adjacent files, press and hold the **Shift** key, and click the first and last files in the group. To select non-adjacent files, press and hold the **Ctrl** key and click each one.)
- d With the file(s) you want to delete selected, press the **Delete** key.
- e If you want to delete a directory and all the files it contains, select the directory and press **Delete**. Click **Yes** to confirm the deletion.
- f If the *Confirm Dialog* box appears, click **Yes** to complete the deletion process.

B. Defragmentation: After removing unwanted files from your hard disk, you can improve the disk's efficiency by rearranging how the files are stored. This process is called *Defragmentation*. The time it takes to run *Disk Defragmenter* will vary (~10 minutes to one hour) depending on the size and condition of your hard disk. Defrag your hard disk once every month or so to keep your computer in tip-top shape as follows:

1. Click on **Start**, select **Programs**, select **Accessories**, select **System Tools**, and then click **Disk Defragmenter**.
2. A dialog box appears, asking which disk drive you want to defragment. Select the desired drive from the drop-down list, and click **OK**.
3. Another dialog appears, indicating the percentage of file fragmentation on the disk, and telling you whether or not you need to defragment the disk now.
4. Click on **Start**, and *Defragmenter* starts to defragment the files on the disk.
5. When you get the message saying that defragmentation is complete, click **Yes** to quit *Defragmenter*.

III. Mailbox Management

- A. Checking Your Mailbox Size: Each user has a limit on the amount of disk space allocated for e-mail storage (mailbox) on the network. Therefore, it is important to periodically (we recommend weekly) check you mailbox as follows.
1. Under the **Outlook Shortcuts**, right click on **Outlook Today**.
 2. Click on **Properties**. (Mailbox - User Name Properties window opens.)
 3. Click on the **Folder Size** tab on the bottom left of the window.
 4. Total Size (of the Folders & Sub-folders under this mailbox) is listed.
- B. Deleting a Message After Reading It: If you don't need to keep a message after you've read it, you can delete that message. E-mail messages certainly have a tendency to accumulate over time, so it's a good idea to keep your Inbox as clean as possible. After reading a message in the *Message Window*, you can delete the message by clicking the **Delete** button on the toolbar, or by pressing **CTRL + D**. The message is moved to the *Deleted Items* folder. Items in the *Deleted Items* folder are not immediately removed from your system. You should remember the following things about deleted items:
1. Items in the *Deleted Items* folder can be recovered by moving them back to the *Inbox* or another folder.
 2. To empty the *Deleted Items* folder, open the **Tools** menu and choose **Empty "Deleted Items" Folder**.
 3. To have Outlook automatically empty the *Deleted Items* folder after each Outlook session, open the **Tools** menu and choose the **Options** command. Under the **Other** tab, check the box labeled *Empty the Deleted Items folder upon exiting*. Then click on the **Advanced Options...** button. The *Advanced Options* dialog box will open. Click on the check box next to the options you want to select. (e.g., Warn before permanently deleting items; Provide feedback with sound). Click **OK** until all open dialog boxes are closed.
 4. After the items are deleted from the *Deleted Items* folder, they can't be removed. If you have configured Outlook to automatically empty the *Deleted Items* folder upon exiting, it's up to you to check that no important items are in that folder before you exit Outlook.

IV. E-mail Attachment Management

How to save the attachments as files?

- A. Saving the Attachments From a Message: You can save the e-mail attachment on your local hard drive or network as follows:
1. Open the **File** menu and choose the **Save Attachment** command.

2. If the message contains more than one attachment, the *Save All Attachments* dialog box appears. Select the attachments that you want to save in the same location then click **OK**.
 3. The *Save Attachment* dialog box appears. Select the location where you want to save the attachment and click **Save**.
- B. Checking for Viruses on Attachments: Since the e-mail attachment are the common sources for computer viruses, never open an attachment without checking for viruses as follows:
1. Right Click on the saved *Attachment file*, and click on **Check for Virus** option.

V. Network Password Management

How to change your password?

- A. Changing your Network Password for Windows 95/98 Workstations: Your network password is case-sensitive. If you are sure you typed the correct password but it was rejected, check make sure the **Caps Lock** key isn't turned on, and type the password again. It is better to change your passwords periodically as follows:
1. Click on **Start**, select **Settings**, and choose **Control Panel** from the submenu.
 2. Double-click the **Passwords** icon.
 3. Click on the **Change Other Passwords** button.
 4. Select the **Microsoft Networking** for which you want to change your password.
 5. Click the **Change** button.
 6. Type your *old password*, and then type a *new password*. Type the new password again to confirm it, and click **OK**.
 7. Click **OK** when Windows confirms the change, and click Close.

VI. Windows 95/98 Password Protection

The Screen Saver Password is a useful protection against prying eyes, but doesn't provide a high level of security similar to Windows NT workstation. To use the screen saver to protect your computer from unauthorized use:

1. Right click a blank area of the Windows desktop.
2. Click **Properties**. (*Display Properties* window appears.)
3. Click on **Screen Saver** tab to display its options.
4. Click on **Password Protected** option.
5. Click on the **Up** or **Down** arrow next to the **Wait:** box to set the amount of time before the screen saver starts.

6. Click on **Change** button.
7. Type your password in the **New Password** and **Confirm New Password** text boxes, and click **OK**.

(Caution: If you forget your *Screen Saver Password*, you have to reboot your system and reset your *Screen Saver Password*. We suggest you to have the same *Network Password* as your *Screen Saver Password*. If it is the case, do not forget to change your *Screen Saver Password* when ever you change/reset your *Network Password*.

Index

Administrators	7, 8
Anti-virus Software	6, 7
Attachments	7-10, C-3, C-4
Deleted Items	9, 10, C-3
Directorate of Information Technology	2
Directorate of Information Technology (DIT)	1
Electronic Mail (E-mail)	2
File Transfer Protocol (FTP)	6
Freedom of Information Act (FOIA)	2
Hacking	4, A-12
Hatch Act	4
Help Desk	5-7, B-2
Information Technology (IT)	1
Internet	1-4, 7-10, A-12, C-2
Mailboxes	8
Monitoring	2, 7, 8, 11
Network Home Directory	7, A-12, C-1
Office of Management Data Systems (OMDS)	1
OSHANET	Cover Page, 1-11, B-2
Passwords	5, 6, C-4
Personal Use	3, 4, 10
Privacy	2
Security	1, 4-7, 9, A-12, C-4
Software	2, 3, 5-7, 9, 10
Spamming	A-12
Storage	2, 7-9, C-1, C-3
Trojan Horse	4, A-12
Violations	2, 11
Viruses	4, 6, 7, 10, A-12, C-4
Worm	A-2