Republic of the Philippines
DEPARTMENT OF SCIENCE AND TECHNOLOGY

NOV 2 5 2003

DOST Administrative Order No. 0 1 2
Series of 2003

SUBJECT: **DOST ICT USAGE AND SECURITY POLICY**

In view of the approval of the DOST ICT Usage and Security Policy by the DOST Management Committee, its adoption in the DOST System is hereby promulgated.

All concerned officials are hereby directed to ensure its efficient implementation in accordance with the guidelines (attached).

This Order shall take effect immediately.

ESTRELLA F. ALABASTRO
Secretary

Postal Address: 2/F, DOST Main Building, General Santos Avenue
Bicutan, Taguig, Metro Manila
Cable Address: Science Manila

Telephone Nos.: (63-2) 837–20–71 to 82
Fax No.: (63-2) 837-29-37
URL: http://www.dost.gov.ph

Republic of the Philippines
Department of Science and Technology

ICT Usage and Security Policy

October 2003

Table of Contents

Section I.	POLICY STATEMENT	1
Section II.	SCOPE OF THE POLICY	1
Section III.	DEFINITION OF TERMS	1
Section IV.	GENERAL NETWORK ACCESS POLICY	1
Section V.	NETWORK SECURITY MANAGEMENT	2
Section VI.	SYSTEM ACCESS REQUIREMENTS	3
Section VII.	REMOTE DIAL-UP SERVICES	3
Section VIII.	VIRUS PREVENTION	4
Section IX.	E-MAIL ACCOUNTS	4
Section X.	PRIVACY AND LOGGING	4
Section XI.	USER RESPONSIBILITIES	5
Section XII.	PROHIBITED ACTS AND USES OF THE ICT RESOURCES	5
Section XIII.	TOLERATED USE	8
Section XIV.	DISCIPLINARY ACTION	8
Section XV.	ENFORCEMENT PROCEDURES	9
Section XVI.	WAIVER AND DISCLAIMER	10
Section XVII.	EFFECTIVITY	10

ANNEX A. DEFINITION OF TERMS
ANNEX B. OFFENSES AND EQUIVALENT ADMINISTRATIVE OFFENSES

Republic of the Philippines
Department of Science and Technology

ICT Network Usage and Security Policy

Section I. POLICY STATEMENT

1 All Information and Communications Technology (ICT) facilities and resources of the Department of Science and Technology (DOST) are valuable assets and must only be used to perform work-related duties or officially authorized activities.

2. The use of these ICT facilities and resources is a privilege granted by the DOST. All users are directed to use these ICT facilities and services properly within legal and proper boundaries.

3. Any offense or violation of this policy will be dealt with according to Philippine laws and the rules and regulations of the Civil Service Commission.

Section II. SCOPE OF THE POLICY

1. Personnel Covered. This policy applies to all personnel employed by or contracted by the DOST, its agencies and offices, including its trainees.

2. Items Covered. This policy covers the proper use of the ICT facilities and resources of the DOST, which includes all ICT equipment, software, data in all formats, accessories, networking facilities and services whether central or remote.

3. Documents Comprising the Policy. This Policy document consists of the following documents:

	Document	Contents
a.		Policy statements.
b.		Definition of Terms.
c.		Usage Offenses and Equivalent Administrative Offenses

Section III. DEFINITION OF TERMS

The Definition of Terms found in Annex A shall be used, and shall form an integral part of this Policy. The Definition of Terms may be updated from time to time to reflect new equipment and services, and new perspectives in the use of ICT facilities and resources.

Section IV. GENERAL NETWORK ACCESS POLICY

1 Use of ICT Facilities and Resources. Agency network facilities and resources are to be used for work-related activities and functions. This policy is to ensure the effective use of networking resources and shall equally apply to all employees.

2. Exception. Agency Heads may approve the use of network resources beyond the scope of this access policy under the following conditions:

    a. The intended use of network resources serves a legitimate Agency interest.

    b. The intended use of network resources is for the individual's educational purposes and development.

Section V. NETWORK SECURITY MANAGEMENT

1 Components of the Network. The network components are the following:

    a. All cabling used to carry voice and data.

    b. All devices to control the flow of voice and data communication, such as hubs, routers, firewalls, switches, etc.

    c. Monitors, storage devices, modems, network cards, memory chips, keyboard, cables and accessories.

    d. All computer software: applications, utilities, tools, and databases.

    e. All output devices including printers, fax machines, CD writers, etc.

2. Authority to Install, Upgrade, Delete. The authority and responsibility to install, upgrade or modify any hardware or software rests solely on the Network Management Group (NMG) or personnel authorized by the Agency Head to do so.

    a. Software Upgrades. The following are considered modifications: installing patches provided by the software supplier or downloaded from the internet; installing anti-virus s; installing new versions of the operating system or any office applications, e.g., word-processing or spreadsheet applications.

    b. Systems Inspection and Deletions. The NMG or authorized personnel may delete files or software that are unauthorized, provided that this deletion or modification is done in the presence of the user or his immediate supervisor.

    c. Hardware Maintenance. The NMG or authorized personnel is the only authorized entity to inspect any ICT equipment. Equipment, software or services under warranty may not be altered or inspected by unauthorized personnel.

    d. Equipment Movements. The NMG or authorized personnel is the only authorized entity to move equipment from one location to another, except for mobile computers such as notebooks, laptops, and wireless user devices.

    e. Authority to Secure Equipment and Services. The NMG, or the authorized personnel, has the responsibility to maintain security of Internet resources against intrusion and destruction. They are tasked to research security and disaster recovery matters to maintain a high degree of reliability of the systems.

Section VI. SYSTEM ACCESS REQUIREMENTS

Access Privilege. All qualified users of the DOST ICT facilities shall be issued a unique login name and password to gain access to network resources.

2. Passwords.

   a. Confidentiality. It is the responsibility of the employee to ensure that his/her password remains secret and secure. The employee shall not share it with other individuals. The exception is when an employee surrenders his/her password if requested to do so in the presence of his/her direct supervisor.

   b. Standards. Passwords are to be a minimum of eight (8) alphanumeric characters. Passwords should not consist of common words or variations on the employee's name, login name, server name, or agency name.

   c. Maintenance. Each user is encouraged to periodically change his/her password in order to have a secured network environment, although the employee has the option to retain his/her password or not when prompted.

3. Username. The NMG shall issue the standardized naming convention and format of usernames to be adopted.

4. Security Responsibility. The Agency reserves the right to hold the employee liable for damages caused by the employee's failure to protect the confidentiality of his of her password in accordance with the above guidelines.

Section VII. REMOTE DIAL-UP SERVICES

1. Remote Access Privileges. DOST provides remote connection to the DOST resources and to the Internet, subject to the following conditions:

   a. User-provided Equipment. The user shall be responsible for providing the computer, modem and phone line, and all accessories to connect to the DOST remote access services.

   b. User Account and Password. Users shall be provided a user account and password to connect to the remote services. It is the responsibility of the user to keep this user account and password confidential, and to keep all information regarding remote network access confidential. Propagating remote access details is considered a security breach and grounds for immediate dismissal.

2. Limits of Use.

   a. Time Connection. Remote dial-up services shall be available for Internet connection only from 6:00 P.M. to 7:00 A.M. daily.

   b. Availability. Connection is dependent on the availability of free phone lines. The remote services shall be on a *"First Come First Served Basis"* since there are more remote user accounts than phone line connections.

c. Duration. Users are granted a maximum of thirty (30) hours total connect time per month.

Section VIII. VIRUS PREVENTION

1 Authorized Anti-Virus Program. No anti-virus programs are allowed to be installed in any DOST computer, whether stand-alone or networked, except those prescribed by the Network Management group or the network personnel authorized by the Agency Head.

2. Installation. Users may install these anti-virus programs subject to instructions, which shall be made available by the NMG or the authorized personnel. The installation can be made through the network.

3. Announcements and Updates. The NMG is responsible for the daily updating of the anti-virus program located in the servers. The NMG shall periodically give advisories to all DOST users to keep them informed of the best practices to combat viruses.

4. User Responsibility in Anti-Virus Protection. It is the responsibility of the user to keep his/her anti-virus programs updated regularly - at least every week.

Section IX. E-MAIL ACCOUNTS

1 DOST E-mail Privileges. The DOST grants e-mail accounts to its employees, subject to the following conditions:

   a. The employee shall not use e-mail for purposes that are illegal, immoral, or disallowed by the DOST.

   b. Since the e-mail disk space is limited, the Agency Head shall indicate the maximum allowable load for e-mail messages and attachments. It is the responsibility of the user to maintain his/her e-mail files, i.e., to delete unwanted files, and to save those that are required for archiving.

2. Responsibility of Maintenance. The NMG shall be responsible of giving the e-mail privileges.

3. Other E-mail Accounts. The user may use non-DOST e-mail services, provided the use of these mail services are consistent with the duties and responsibilities of the employee.

4. Surrender and Waiver. It is understood that e-mail privileges including the disk files containing the e-mail files of the user are surrendered upon separation, termination, resignation, retirement or other circumstances deemed legal by the DOST, and shall be subjected to clearance procedures.

Section X. PRIVACY AND LOGGING

1. Ownership and Right to Monitor. All agency ICT facilities and resources are owned by DOST. The Agency reserves the right to monitor and/or log all network-based activity. The employee is responsible for surrendering all passwords, files, and/or other required

resources if requested to do so in the presence of his/her Agency Head, or person designated by the Agency Head.

2. Implied User Agreement to Terms and Conditions. By logging-in to the DOST ICT facilities, the user agrees to the terms and conditions of this Policy.

Section XI. USER RESPONSIBILITIES

1. Reporting of Troubles or Problems / User Cooperation. Users should report suspected abuse, especially any damage to, or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions. Users should cooperate with system administrators in any investigation of system abuse.

2. Contact Person or Unit. Exception and trouble reports must be made to the NMG so that appropriate action can be taken to solve the problem.

Section XII. PROHIBITED ACTS AND USES OF THE ICT RESOURCES

1. General Principles in Proper Use of ICT Resources.

    a. A user may access only those services and parts of the ICT System that are consistent with his/her duties and responsibilities. The ICT System should be used in accordance with its authorized purpose.

    b. The following uses and acts, discussed in the following paragraphs, are considered violations in the use of the DOST ICT facilities and resources:

        i. Uses contrary to laws, customs, mores and ethical behavior;
        ii. Uses for personal benefit, business, or partisan activities;
        iii. Acts that damage the integrity, reliability, confidentiality and efficiency of the ICT System;
        iv. Acts that encroach on the rights of other users; and,
        v. Acts that violate privacy.

2. Uses Contrary to Laws, Customs, Mores, and Ethical Behavior

    a. Criminal Use. Users should not use the DOST Network Information resources for criminal activities.

    b. Use of Copyrighted Material without Attribution. Prohibited acts include but are not limited to:

        i. Copying, reproduction, dissemination, distribution, use, importation, removal, alteration, substitution, modification, storage, uploading, downloading, communication, publication or broadcasting of copyrighted material not properly attributed.

        ii. Infringement of intellectual property rights belonging to others through the use of telecommunications networks, which is a criminal offense under Section 33(b) of the Electronic Commerce Act.