



Acceptable Use Policy (AUP)

Philippine Research, Education and Government Information Network (PREGINET)

1.0 Overview

This AUP is implemented in conjunction with the Department of Science and Technology's (DOST's) ICT Usage and Security Policy.

2.0 About this Document

The ASTI, as DOST's R&D arm in ICT and Electronics is responsible for building, operating and maintaining science infrastructures in support of the national R&D agenda. In 1999, PREGINET was started, and since then, advanced research and education network technologies have become one of the focus areas of DOST-Advanced Science and Technology Institute (DOST-ASTI). The Agency continues to operate and maintain PREGINET, which has now become an essential service of the Institute.

This AUP is intended to set guidelines for all users of PREGINET on what is allowed and not allowed over the network, in order to protect against illegal or damaging actions by individuals, either knowingly or unknowingly. As a Research and Education Network (REN), the purpose of PREGINET is to connect academic, research and government¹ institutions to facilitate and support scientific research aligned with the priorities of the National R&D Agenda. It is a shared responsibility of all users of the network to be aware of these guidelines and to conduct their activities accordingly.

3.0 Definition of Terms

- 3.1 Research and Education Network (REN):** A high-speed network that runs high-performance, high-bandwidth applications that support scientific breakthroughs in research, and which serve as testbeds for innovation. Over these networks, large data transfers are carried out across continents, enabling cross-institution and cross-country collaboration on high-impact research activities.
- 3.2 Government Network (GovNet):** Includes National Government Agencies (NGAs) and their attached agencies and regional offices connected through the Integrated Government Philippines (iGovPhil) Project, and maintained by the Department of Information and Communications Technology (DICT).
- 3.3 Integrated Government Philippines (iGovPhil):** The iGovPhil Project was launched on 28 June 2012. It seeks to achieve a higher level of e-government, or the application of information and communications technology (ICT) to rationalize government operations and improve the delivery of services to the people. The project was jointly implemented by the DOST-Information and Communications Technology (DOST-ICTO) and DOST-ASTI until its transition to the DICT in 2017.
- 3.4 Network Resources:** Hardware devices such as, but not limited to, routers, switches, media converters, servers; software and tools; IP addresses and other ICT facilities that are part of the PREGINET infrastructure and that are needed to operate a REN.
- 3.5 Agreement:** Memorandum of Agreement or MOA executed between DOST-ASTI and PREGINET Partner that provides the provisions and conditions for PREGINET connectivity.

¹ The Department of Information and Communications Technology (DICT) operates the Government Network (GovNet). A small number of National Government Agencies (NGAs) that have research mandates or have collaboration with the DOST-ASTI are connected to PREGINET.

4.0 Purpose

The purpose of this policy is to lay out the acceptable use of network resources of PREGINET to ensure the efficiency, integrity, security and reliability of the REN. Inappropriate use of such resources exposes PREGINET to various risks and vulnerabilities including all forms of cyber-based attacks, hacking, compromises of the network systems and services, data leakage and legal issues.

5.0 Scope

- 5.1 This policy applies to all PREGINET-connected institutions and their employees that use PREGINET-provided network resources and connectivity.
- 5.2 This policy applies to all PREGINET-owned equipment, including those deployed in other agencies, or any device accessing the network.

6.0 Policy

6.1 General Conditions of Use

- 6.1.1 While PREGINET network administration espouses a reasonable level of privacy, partners and users should be aware that PREGINET is intended to support scientific research and development activities only. Partners and users are expected to be responsible in using PREGINET-provided resources in an efficient, effective, ethical and lawful manner.
- 6.1.2 For security and network maintenance purposes, as well as network incidents, authorized personnel that are part of the PREGINET Operations Team may monitor equipment, systems and network traffic at any time.
- 6.1.3 PREGINET reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

6.2 Monitoring, Security and Enforcement

While not obligated to perform investigations, the PREGINET Operations Team may conduct the following monitoring, security and enforcement activities in accordance with the terms of this AUP:

- 6.2.1 The demarcation point of PREGINET is up to the customer premise equipment (CPE) installed in the partner's premises. From the CPE, any network component going into the partner's local area network (LAN) is the responsibility of the partner. It is understood that monitoring and security activities of PREGINET will be up to the CPE.
- 6.2.2 Investigate violations to the AUP and misuse of PREGINET-provided resources.
- 6.2.3 Investigate and help prevent security threats, fraud, or other illegal, malicious or inappropriate activity.
- 6.2.4 Remove, suspend access to, modify or terminate the provision of resource that are found to be in violation of this AUP or any other agreement that PREGINET has with an agency connected to PREGINET. In such case, a one-month notice prior to the suspension or termination will be sent to the partner, unless the situation necessitates immediate action to disconnect a device on the network.
- 6.2.5 Should a request for reconsideration be provided by the partner, such request will be subject to a thorough evaluation and approval/disapproval process.
- 6.2.6 In the case of investigation carried out by a third-party or agency authorized to conduct or lead such investigation, suspension or termination of PREGINET service shall be put on hold until the investigation is concluded, unless the situation necessitates immediate action to disconnect a device on the network.

6.3 Prohibited Use and Content

The following activities are, in general, prohibited. Under no circumstances is a PREGINET-connected partner or user authorized to engage in any activity that is illegal under national or

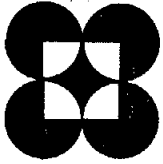
international law utilizing PREGINET-provisioned resources. The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of prohibited use and content:

- 6.3.1 Unrelated to R&D activities, unless otherwise specified in an Agreement;
- 6.3.2 In violation of any local, national or international statute, regulation, rule, order, treaty, or other pertinent laws;
- 6.3.3 Abusive, deceptive, pornographic, obscene, defamatory, slanderous, offensive, or otherwise inappropriate or illegal;
- 6.3.4 In violation of or is encroaching on the rights of others, including, but not limited to, infringement or misappropriation of any intellectual property or proprietary rights of another;
- 6.3.5 An impersonation of any person or entity or otherwise misrepresents a PREGINET user's affiliation with a person or entity;
- 6.3.6 An interference, disruption, or degradation to the PREGINET services, other PREGINET users' access to the network and usage of network services, or equipment or networks connected to PREGINET;
- 6.3.7 A means to violate the security and integrity of a system, including, but not limited to:
 - 6.3.7.1 Accessing or using any system, whether through hacking, password mining, or any other means, including attempts to probe, scan, or test the vulnerability of a system or to breach any security or authentication measures used by a system, without permission granted by the PREGINET Operations Team;
 - 6.3.7.2 Monitoring data or traffic on a system without permission granted by the PREGINET Operations Team;
 - 6.3.7.3 Forging packet or email headers, or any part of a message describing its origin or route;
 - 6.3.7.4 Intentional uploading of malicious content (such as those that contains viruses, worms, corrupt files, trojan horses, or other forms of corruptive code, or any other content that may compromise the services);
 - 6.3.7.5 Hacking, destabilizing, or adapting the PREGINET services, or altering another website to falsely imply its affiliation with the PREGINET;
 - 6.3.7.6 Activities that connect to any users, hosts, or networks where PREGINET users do not have permission to communicate with, i.e., users, hosts, or networks;
 - 6.3.7.7 Monitoring or crawling a system so that such system is impaired or disrupted;
 - 6.3.7.8 Intentionally interfering with the proper functioning of any system, including any deliberate attempt to overload a system by any means (e.g. distributed denial-of-service attacks, etc.); and
 - 6.3.7.9 Operating network services like open proxies, open mail relays, or open recursive domain name servers.

7.0 Penalties

Any proven violations of this policy shall be dealt with on a case-to-case basis. Depending on the impact of the incident to the operations and integrity of the network, appropriate sanctions may include network removal, access revocation, termination of services, and administrative or criminal prosecution.

Applicable Offenses and Equivalent Administrative Offenses specified in ***Annex B of DOST ICT Usage and Security Policy*** shall be adopted as appropriate.



Republic of the Philippines
DEPARTMENT OF SCIENCE AND TECHNOLOGY

NOV 25 2003


DOST Administrative Order No. 012
Series of 2003

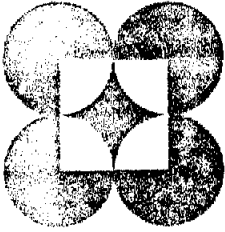
SUBJECT: DOST ICT USAGE AND SECURITY POLICY

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



Republic of the Philippines
Department of Science and Technology

ICT Usage and Security Policy

October 2003

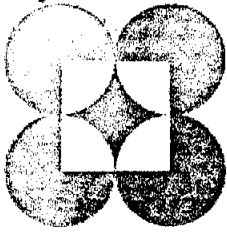
Table of Contents

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

L. T. del Rosario



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:

<u>Document</u>	<u>Contents</u>
a. Main Policy Document	Policy statements.
b. Annex A	Definition of Terms.
c. Annex B	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

1. 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

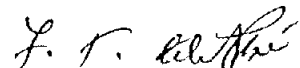
1. Authorized Anti-Virus Program. No anti-virus programs are allowed to be installed in any DOST computer, whether stand-alone or networked, except those prescribed by the Network Management group or the network personnel authorized by the Agency Head.
2. Installation. Users may install these anti-virus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

c. Cheating. Prohibited acts include but are not limited to:

- i. Copying a computer file that contains another person's work and submitting it for one's own credit, or, using it as a model for one's own work, without the permission of the owner or author of the work;
- ii. Submitting the shared file, or a modification thereof, as one's individual work, when the work is a collaborative work, or part of a larger project.

3. Uses for Personal Benefit, Business or Partisan Activities

- a. Commercial Use. Use of the ICT System for commercial purposes, and product advertisement, for personal profit, unless permitted under other written Office policies or with the written approval of a competent authority.
- b. Use of the ICT System for any partisan political activities. Use of ICT resources for religious or political lobbying, for disseminating information or gathering support or contributions for social, political or cause-oriented group, which are inconsistent with the activities of the Agency of the Department.
- c. Games and Entertainment. Use of ICT resources to play games, watch video, or any activity unrelated or inappropriate to the duties and responsibilities of the user, especially during office hours.

4. Acts that Damage the Integrity, Reliability, Confidentiality and Efficiency of the ICT System.

- a. Destruction, deletion, removal, modification, or installation of any computer equipment, peripheral, operating system, disk partition, software, database, or other component of the ICT System;
- b. Connection of any computer unit or external network to the ICT System without the permission of the NMG or the Agency Head.
- c. Acts that attempt to crash, tie up, or deny any service on the ICT System, such as, but not limited to: sending of repetitive requests for the same service (denial-of-service); sending bulk mail; sending mail with very large attachments; sending data packets that serve to flood the network bandwidth.
- d. Concealment, deletion, or modification of data or records pertaining to access to the ICT System at the time of access, or alter system logs after such access for the purpose of concealing identity or to hide unauthorized use.
- e. Concealment of identity, or masquerading as other users when accessing, sending, receiving, processing or storing through or on the ICT System.

5. Acts that Encroach on the Rights of Other Users

- a. Sending Unsolicited E-mail. Sending unsolicited mail such as chain-letters, advertisements, jokes, trivia, announcements to non-official groups or activities, offers, inquiries, and the like (spamming);



- b. Morally Offensive and Obscene Use. Accessing, downloading, producing, disseminating, or displaying material that could be considered offensive, pornographic, racially abusive, culturally insensitive, or libelous in nature.
- c. Sending Fraudulent and Harassing Messages. Sending messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of the DOST.
- d. Acts that interfere with or disrupt other computer users such as, but not limited to: sending messages through pop-up screens; running programs that simulate crashes; running spy ware to monitor activities of other users.

6. Acts which Violate Privacy

a. Hacking, Spying or Snooping.

- i. Accessing, or attempting to gain, access to archives or systems that contain, process, or transmit confidential information. Authorized users should not exceed their approved levels of access, nor should they disclose confidential information to others.
- ii. Decrypting, attempting to decrypt, or enabling others to decrypt such information which are intentionally decrypted, password-protected, or secured. Encrypted data are considered confidential, and include, but not limited to: passwords, digital keys and signatures.
- iii. Re-routing or capture of data transmitted over the ICT System.
- iv. Accessing, or attempting to access, restricted portions of the system, such as e-mail lists, confidential files, password-protected files, or files that the user has no authorization to open or browse.

b. Unauthorized Disclosure.

- i. Copying, modification, dissemination, or use of confidential information such as, but not limited to: mailing lists; employee directories of any sort; DOST operations data; research materials, in whole or in part, without the permission of the person or body entitled to give it.
- ii. Searching, or providing copies of, or modifications to, files, programs, or passwords belonging to other users, without the permission of the owners of the said files, programs or passwords.
- iii. Publication on mailing lists, bulletin boards, and the World Wide Web (www), or dissemination of prohibited materials over, or store such information on, the ICT System. Prohibited materials under this provision include but are not limited to the following:

1. Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;
2. Any material that enables others to gain unauthorized access to a computer system. This may include instructions for gaining such access, computer code, or other devices. This would effectively preclude displaying items such as "Hackers Guides", etc.
3. Any material that permits an unauthorized user, who has gained access to a system, to carry out any modification of the computer programs or data stored in the system; and
4. Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system.

7. Acts that Waste Resources

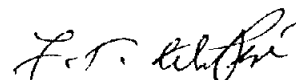
- a. Printing excess copies of documents, files, data, or programs.
- b. Repeated posting of the same message to as many newsgroups or mailing lists as possible, whether or not the message is germane to the stated topic of the newsgroups or mailing lists targeted.
- c. Sending large unwanted files to a single email address.

Section XIII. TOLERATED USE

1. Tolerated Use. Some ICT use, though unofficial, may be tolerated. These are considered privileges that may be revoked at any time. They include:
 - a. The use of email for personal communication;
 - b. The use of instant messaging applications; and,
 - c. The use of computers to play compressed audio files or audio CDs.
2. Update to "Tolerated Uses" of ICT Facilities. The DOST management may, from time to time, issue a list classifying certain types of use under the category of "Tolerated Use". This list shall form part of this Policy and will be considered binding to all users.

Section XIV. DISCIPLINARY ACTION

1. Violations. Improper use of ICT resources is subject to penalties. The Agency Head may, upon the recommendation of the investigative body, put a preventive suspension to the Internet and network privileges of the offender/suspected violator.
2. Applicable Laws. All Disciplinary Action proceedings shall follow the Civil Service Commission Uniform Rules and Regulations on Administrative cases, and/or legal action provided by applicable Philippine laws.



3. Penalties for Non-DOST Personnel. Any non-DOST personnel found guilty violating any of the provisions set forth in this Policy, will be barred from entering any DOST premises. The employee who gave permission to the visitor to access the DOST network will also be held liable for all the violations that the visitor may commit.
4. Penalties. In addition to the filing of an Administrative case and sanctions that will be filed against the violators, appropriate charges will be filed in court if offenses are punishable under the E-commerce Law or any other applicable Philippine Laws.

Section XV. ENFORCEMENT PROCEDURES

1. Implementing Body. The Implementing Body shall refer to the Body that shall be responsible for enforcing this ICT Usage and Security Policy. Each Agency Head / Regional Head shall constitute the Implementing Body which should include personnel from the Information Technology (IT) unit and from the Human Resources unit.
2. Jurisdiction of the Implementing Body on Investigation.
 - a. Upon receipt of a report or complaint of misuse, the implementing body shall conduct an investigation on the matter.
 - b. This group shall have the following authority:
 - i. To summon the subject of the complaint to provide information.
 - ii. To call and interview potential witnesses;
 - iii. To inspect the user's files, diskettes, tapes, e-mail account and/or other computer-accessible storage media, or authorize systems administrators to perform this inspection under its supervision;
 - iv. To retain, as evidence, copies of user files or other data that may be relevant to an on-going investigation;
 - v. To extend the suspension or restriction of a user's computing privileges for the duration of the investigation, or as may be deemed necessary to preserve evidence and protect the system and its users;
 - c. The implementing body shall submit the results and recommendations to the Agency Head for appropriate action.
3. Appropriate Action. If the implementing body has persuasive evidence of misuse of ICT resources, and if that evidence points to the computing activities or the computer files of an individual, the Agency Head shall pursue appropriate actions as provided for the Uniform Rules on Administrative Cases in the Civil Service (CSC Resolutions No. 99-1936).
4. Filing of Charges. In cases where there is evidence of serious misconduct or possible criminal activity, appropriate charges shall be filed by the Agency Head with the proper authorities. This, however, does not prohibit any aggrieved party or complainant other

than the Agency Head from instituting the filing of charges with the appropriate authorities.

5. External Legal Processes. The DOST Network does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, DOST may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources. Use of the DOST computer resources and network is granted subject to existing Philippine laws and regulations.

Section XVI. WAIVER AND DISCLAIMER

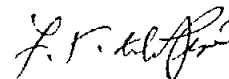
1. Disclaimer. While the DOST takes careful steps to provide reliable and professional services in its network, DOST does not guarantee, nor does it provide any warranties, as to the operating characteristics of its ICT resources and facilities to any of its users.
2. Waiver. DOST shall not be responsible for any loss or damage, whether direct or indirect, implied or otherwise, that may arise from the use of the DOST ICT facilities and resources by any person or entity.

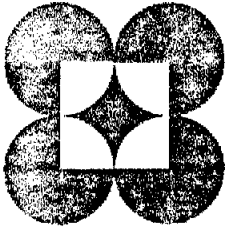
Section XVII. EFFECTIVITY

1. Effectivity. This policy is effective upon the approval of the Department Secretary.
2. Amendments. The Department may amend or modify this policy to maintain its applicability. These amendments or modifications shall form part of the overall DOST ICT Network and Security Usage Policy, and will be considered binding on all users.

Approved this 19th day of November 2003.


ESTRELLA F. ALABASTRO, Ph.D.
Secretary





Republic of the Philippines
Department of Science and Technology

ICT Usage and Security Policy

October 2003

Annex A. DEFINITION OF TERMS

Access – To connect to the Internet; to “log-in”; to be in the Internet to browse, retrieve data, communicate via e-mail. Also, to connect to a computer system or server that enables one to get online. Access to the internet can be through a dial-up (DUP) connection to an Internet Service Provider (ISP) via a modem, or through network such as an office LAN.

Account – A unique identifier which may consist of an account name or account ID, and a password. This allows the account holder to access network facilities, either a local area network (LAN) or the Internet.

Agency – The Department of Science and Technology; or any of its agencies or institutions.

Alphanumeric – Characters that consist of letters, numbers, punctuation, and symbols. These consist of the following: letters of the alphabet A-Z and a-z; numbers 0-9; the characters ! @ # \$ % ^ & * () _ - + = { [] } | \ : ; " ' < . > . ? / ~ ` . These are found on a standard keyboard.

Authorized users - Refers to one or more of the following: (1) current employees of DOST either permanent, casual or contractual; (2) individuals connecting to a public information service; or (3) others whose access and usage does not interfere with other authorized users' access to resources. In addition, a user must be specifically authorized to use a particular computing or network resource by the DOST Network responsible for operating the resource.

Bandwidth – The number of bits of information that can move through a communications medium in a given amount of time; the capacity of a telecommunications circuit/network to carry voice, data, and video information. Typically measured in thousand bits per second or kilobits/sec (Kbps) and million bits per second or megabits/sec (Mbps). Bandwidth from public networks is typically available to business and residential end-users in increments from 56kbps to T-3. Bandwidth may be likened to the size of a water pipe. The larger the diameter of a pipe, the more water that can flow through at any given time.

Computer Virus – A program which replicates itself on computer systems by incorporating itself into other programs that are shared on a system. Most often thought of as “malicious” viruses are best known for “spreading overnight from one computer to millions of others around the world” and infecting machines causing them to crash. The following are types of common viruses:

Trojan Horse – This virus enables unauthorized remote computers to access secured network workstations or equipment.

Worms – This form of virus reproduce and run independently, and travel across network connections. A worm infection can result to loss of storage space of the computer unit which leads to computer instability or impairs its function

Confidential information – Refers to data or information which is not intended for general

dissemination. Examples include proprietary technical information, disciplinary case records, administrative records, and the like.

Decryption – The process of transforming cipher text into readable text.

Document – Refers both to the paper and its electronic format.

DOST System – This refers to DOST Central Office, its attached agencies, regional offices and the provincial Science and Technology Centers.

Electronic Mail (E-mail) – Electronically transmitted mail.

Email “bombing” – The repeated sending of an identical email message to a particular address.

Email “spamming” – A variant of bombing; it refers to sending email to hundreds or thousands of users, or to lists that expand to that many users. Email spamming can be made worse if recipients reply to the email, causing all the original addresses to receive the reply.

Encryption – A way to make data unreadable to everyone except the receiver. This is done with the use of formula, called encryption algorithm. It translates plain text into an incomprehensible cipher text.

Hacking – Gaining unauthorized access to computer systems and data.

ICT Facilities and Resources – Includes computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment; software, databases and other data files; and, facilities such as data centers, cabinets, and related peripherals that are owned, managed, or maintained by DOST. For purposes of this Policy, any other equipment, computer unit or external network, when attached to, or used to access and/or interact with any component

of, the IT System may also be considered part of the ICT System.

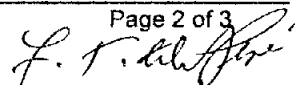
Internet – A system of linked computer networks, global in scope, that facilitates data communication services such as remote login, file transfer, electronic mail, and newsgroups. The Internet is a way of connecting existing computer networks that greatly extends the reach of each participating system.

Internet Service Provider (ISP) – A company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. The ISP is different from the provider of the link, which is usually a telephone company (Telco).

IP Address – A numeric address that is given to servers and users connected to the Internet. For servers it is translated into a domain name by a Domain Name Server a.k.a. the DNS. When a user is “online”, it is assigned an IP address by the Internet Service Provider (ISP). This IP address may be the same every time one logs-on (called the static IP) or it can change and be assigned each time one connects based on what’s available (dynamic IP).

IP spoofing – A technique used to gain unauthorized access to computers, whereby the hacker sends messages to a computer with an IP address indicating that the message is coming from a trusted port. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted port and then modify the packet headers so that it appears that the packets are coming from the port.

Local Area Network (LAN) – A network that connects computers in a small pre-determined area like a room, a building, or a set of buildings. LANs can also be connected to each other via telephone lines, and radio waves. Workstations and personal computers in an office are commonly connected to each other with a LAN. These allow them to



send/receive files and/or have access to the files and data. Each computer connected to a LAN is called a node.

Modem (MOdulator, DEModulator) – Modem comes from the 2 words Modulation & Demodulation. A Modem converts information from Analog to Digital & vice versa. Digital information is represented in a series of 1's & 0's. It is used when one connects to a phone line, which allows the computer to talk to other computers through the phone system. Basically, modems do for computers what a telephone does for humans. Generally there are 3 types of modems: external, PC Card and internal.

Network – A communications system that links two or more computers. It can be as simple as a cable strung between two computers a few feet apart or as complex as hundreds of thousands of computers around the world linked through fiber optic cables, phone lines and satellites.

Private files – refer to information that a user would reasonably regard as private. Examples include the contents of electronic mail boxes, private file storage areas of individual users, and information stored in other areas that are not public, even if no measure has been taken to protect such information.

Public Information Services - These are information retrieval services for the public such as web browsing through the world wide web (WWW) and file transfer (download).

Remote Dial-up Services – Service provided using a computing device linked via communications lines such as ordinary phone lines or wide area networks, to access distant network applications and information.

Router – A communication device between networks that determines the best path between them for optimal performance. Routers are used in complex networks of networks such as enterprise networks and Internet.

Server – A computer that provides a central service to a network, such as: storage of files (data server); location of application software (application server); e-mail services (e-mail server).

System and Network Administrator – Refers to the person designated to manage the particular system assigned to her/him, to oversee the day-to-day operation of the system, or to preliminarily determine who is permitted access to particular facilities and resources of the ICT System, whether hired on a temporary, contractual or permanent basis.

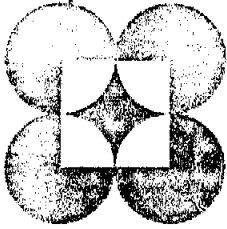
User ID –Also known as a username; it is an identifier, or a handle, for a user on the Internet and is commonly left up to the user to decide what is, although most Web sites or systems will NOT allow the same username to be assigned to two different people.

Users - Unless specified, it refers to the people using the ICT facilities.

Virus – (see Computer Virus)

Workstation - A computer intended for professional or business use, and is faster and more capable than a personal computer. The applications intended to run in workstations are those used by design engineers, architects, graphic designers, and any organization, department, or individual that requires a faster microprocessor, larger amount of random access memory (RAM), and special features such as high-speed graphics adapters.





Republic of the Philippines
Department of Science and Technology

ICT Usage and Security Policy
 October 2003

Annex B. OFFENSES & EQUIVALENT ADMINISTRATIVE OFFENSES

ICT Resources Usage and Network Security Offenses	Equivalent Administrative Offense
1. Commercial Use – Use of DOST ICT Resources for commercial purposes and product advertisement, for personal profit.	Dishonesty or Grave Misconduct
2. Religious or Political Lobbying – Use of DOST ICT Resources for religious or political lobbying. Engaging directly or indirectly in partisan political activities by one holding a non-political office.	Civil service laws, rules and regulations punish engaging in partisan political activities and NOT religious activities. Thus if the DOST ICT Resources were used for religious lobbying, the same is not punishable under this administrative offense. However, the same may be punished under "Conduct Prejudicial to the Best Interest of the Service".
3. Copyright Infringement -- Reproduction, duplication, transmission of copyrighted materials using unlicensed software.	Dishonesty
4. Criminal Use – using the resources for criminal activities.	Grave Misconduct
5. Wiretapping and Traffic Capture – the unauthorized rerouting or capture of traffic transmitted over the voice or data network.	Grave Misconduct
6. Stealing – Stealing of information resources both hardware or software or any part of the network resource.	Grave Misconduct
7. Concealing Access – concealing one's identity or masquerading as another user to access the information resource, send/receive, process, modify or store data on the ICT Resources	Grave Misconduct
8. Password Disclosure – disclosure of user password protected account or making the account available to others without the permission of the System Administrator.	Grave Misconduct
9. Intrusion – attempts to disable, defeat or circumvent any DOST Internet and Security Policy. Unauthorized access to another computer or network thru decrypting, hacking, hijacking, spoofing, etc.	Grave Misconduct
10. Access of other accounts or files within or outside DOST's computers and communication facilities without proper authorization.	Simple Misconduct
11. Copying, renaming or changing information on files/programs that belongs to another user, unless the said user gave permission.	Simple Misconduct
12. Unlawful messages – Use of electronic communication facilities (such as email, talk, chat or systems with similar functions) to send fraudulent, harassing, obscene, threatening or other offensive messages.	Simple Misconduct

F. R. del Rosario

ICT Resources Usage and Network Security Offenses	Equivalent Administrative Offense
13. Offensive Prohibitive Materials – use of computers, printers, electronic mail, data network and other related resources to produce, disseminate, store or display materials which could be considered offensive, pornographic, racially abusive, libelous or violent in nature.	Simple Misconduct
14. Prohibited Materials – Using or encouraging the use of materials that includes instructions to gain unauthorized access (e.g. Hacker's Guide).	Simple Misconduct
15. Unauthorized reading of e-mail or private communications of other users, unless otherwise requested to do so by said users.	Simple Misconduct
16. Misrepresentation in sending e-mail messages	Simple Misconduct
17. Systems Software and Hardware Removal – Unauthorized removal or modification of System software and hardware on any of the DOST ICT Resource.	Simple Misconduct
18. Damaging/Vandalizing – Damaging or Vandalizing any of the Department's ICT Resource including but not limited to all the facilities, equipment, computer files, hardware and software.	Simple Misconduct
19. Unauthorized manipulation/ changing of the DOST ICT Network architecture or setup.	Simple Misconduct
20. Software and Hardware Installation – Unauthorized installation of software and hardware on any of the DOST ICT Resources.	Violation of Reasonable Rules and Regulations
21. Not cooperating with any investigative process in line with computer, network or system abuse.	Violation of Reasonable Rules and Regulations
22. Disclosure of DOST Confidential Information – Transmission of information without authority and proper security clearance. Disclosing or misusing confidential or classified information officially known to him by reason of his office and not available to the public, to further his private interest or give undue advantage to anyone or to prejudice the public interest	
23. Access to lewd sites – A user should not view, transmit, retrieve, save or print any electronic files, images or text which may be deemed sexually explicit or pornographic.	Violation of Reasonable Rules and Regulations
24. Changing of IP Address and Network configuration without the approval of the NMG.	Violation of Reasonable Rules and Regulations
25. Recreational use – No ICT resource must be used for playing any computer game, whether individually or in a multiplayer setting or to be used in watching movies thru VCDs, DVDs and other media.	Violation of Reasonable Rules and Regulations
26. Tolerating or not reporting co-employees who use ICT resources for recreational purposes as mentioned in item no. 25.	Violation of Reasonable Rules and Regulations

OFFENSES & PENALTIES

OFFENSE	PENALTIES
Simple Misconduct	1 st Offense- Suspension for one (1) month and one (1) day to six (6) months; 2 nd Offense- Dismissal
Grave Misconduct	1 st Offense- Dismissal
Dishonesty	1 st Offense- Dismissal
Violation of existing Civil Service law and rules of serious nature	1 st Offense- Suspension for one (1) month and one (1) day to six (6) months; 2 nd Offense- Dismissal
Violation of Reasonable Rules and Regulations	1 st Offense- Reprimand; 2 nd Offense - Suspension for one (1) to thirty (30) days; 3 rd Offense- Dismissal
"Conduct Prejudicial to the Best Interest of the Service"	1 st Offense- Suspension for six (6) months and one (1) day to one (1) year; 2 nd Offense- Dismissal

J. R. del Arco