



Republic of the Philippines
DEPARTMENT OF ENERGY

DEPARTMENT ORDER NO. D02012-01-0001 *w*

**INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) ACCEPTABLE USAGE
AND SECURITY POLICY**

WHEREAS, Republic Act (RA) 8792 or The Electronic-Commerce Act of 2000 is an act providing for the recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes.


WHEREAS, the Department of Energy (DOE) has encountered various issues and concerns related to the use and security of its ICT facilities and resources;

WHEREAS, the DOE ICT Governance Committee, tasked to prepare, implement and ensure sustainability of the ICT plans, programs and projects, has formulated and endorsed the DOE ICT Acceptable Usage and Security Policy;

NOW, THEREFORE, in view of the foregoing premises, the DOE Information and Communications Technology (ICT) Acceptable Usage and Security Policy Guidelines are hereby issued for strict implementation of DOE officials and employees.

This Department Order shall take effect immediately.

Signed and approved on ____ day of _____ 2011 at Fort Bonifacio, Taguig City, Metro Manila.


JOSE RENE D. ALMENDRAS

Secretary



Republic of the Philippines
DEPARTMENT OF ENERGY

JAN 02 2012

IN REPLYING PLS CITE:
SDOE12-000013





Republic of the Philippines
DEPARTMENT OF ENERGY

ICT ACCEPTABLE USAGE AND SECURITY POLICY

TABLE OF CONTENTS

Section I.	Policy Statement	1
Section II.	Objectives	1
Section III.	Scope and Application	1
Section IV.	Definition of Terms	2
Section V.	System Access Requirements	2
Section VI.	ICT Resources Management	3
Section VII.	Virus Prevention	4
Section VIII.	Email Accounts	4
Section IX.	Ownership and Privacy	5
Section X.	User Responsibilities	5
Section XI.	Prohibited Acts and Uses of ICT Facilities and Resources	5
Section XII.	Tolerated Use	9
Section XIII.	Disciplinary Action	9
Section XIV.	Enforcement Procedures	10
Section XV.	Waiver and Disclaimer	11
Section XVI.	Severability	11
Section XVII.	Effectivity and Amendment	12

Annex A. Definition of Terms

Annex B. Offenses and Equivalent Administrative Offenses.



**Republic of the Philippines
Department of Energy (DOE)**

ICT ACCEPTABLE USAGE AND SECURITY POLICY

Section I. POLICY STATEMENT

1. All Information and Communications Technology (ICT) facilities and resources of the Department of Energy are valuable assets of the Government and shall be used in accordance with laws, rules and regulations to ensure efficiency, effectiveness, and responsiveness in the internal operation and management of the Department and the delivery of public service;
2. The use of these ICT facilities and resources is a privilege granted by the DOE to its officials and employees subject to certain conditions. All authorized users shall use these ICT facilities and resources for work related activities and functions and within the legal, ethical and proper boundaries;
3. Any offense or violation of this policy shall be dealt with in accordance to pertinent laws, rules and regulations.

Section II. OBJECTIVES

The Objectives of this Policy are to:

1. Ensure the confidentiality, integrity, efficiency, availability, reliability, and security of DOE information and ICT facilities and resources;
2. Rationalize and optimize the utilization of the DOE ICT facilities and resources;
3. Define User privileges and responsibilities; and
4. Establish processes for addressing Policy violations.

Section III. SCOPE AND APPLICATION

1. This Information and Communication Technology (ICT) Acceptable Usage and Security Policy ("Policy") shall apply to all DOE personnel using in part or in full any DOE ICT resources and facilities including, but not limited to, computers and its peripherals, auxiliary devices, Local Area Network, Application systems, software and hardware;
2. This Policy shall also cover the proper use of the ICT facilities and resources of the DOE, which includes but not limited to all ICT

equipment, software, data in all formats, accessories, networking facilities and services; and

3. All non-DOE Personnel or individuals that are allowed or authorized to use in part any DOE ICT facilities and resources are likewise covered by this Policy. ITMS shall be responsible in disseminating this Policy and conducting orientation for updates/revisions, if any, while the Bureau/Service/Office Director shall be responsible for ensuring compliance of the Users to this Policy.

Section IV. DEFINITION OF TERMS

The Definition of Terms found in Annex A shall be used and shall form integral part of this Policy and shall be interpreted in the context of ICT perspective.

Section V. SYSTEM ACCESS REQUIREMENTS

1. DOE ICT facilities and resources are to be used only for work-related activities and functions.
2. The Secretary or his/her authorized representative/s shall approve the use of ICT facilities and resources beyond the scope of this access policy under the following conditions:
 - a. The intended use serves a legitimate Agency interest, such as Corporate Social Responsibility;
 - b. The intended use is for educational purposes related to the employee's job/functions; and
 - c. The User is a Client of the DOE.
3. Peer network or work group connection shall be allowed provided prior approval from ITMS Director has been obtained.
4. All qualified users of the DOE ICT facilities and resources shall be issued a unique log-in name and password to gain access to network resources.

Passwords

- a. Confidentiality. It is the sole responsibility of the employee to secure his/her password. Should the employee be required to surrender his/her password for whatever legal purpose, the employee is obliged to do so in the presence of his/her direct supervisor.
- b. Standards. Passwords should have a minimum of eight (8) alphanumeric characters and should not consist of common words or variations on the employee's name, log-in 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.

Username

The ITMS shall issue the standardized naming convention and format of usernames to be adopted.

5. The DOE reserves the right to hold the employee liable for damages caused by the employee's failure to protect the confidentiality of his/her password in accordance with the above guidelines.

Section VI. ICT RESOURCES MANAGEMENT

1. All ICT-related projects, activities and requirements of the DOE Bureaus/Services/Offices shall be coordinated to the ITMS.
2. The ITMS shall standardize all ICT resources technical specifications to ensure interoperability and compatibility with existing ICT equipment and systems.
3. All users shall follow the standard file naming conventions to be developed by the ITMS for easy search, storage and retrieval of data/information.
4. All DOE officials, technical and non-technical, and co-terminus employees shall be provided with personal computers each. Messengers, drivers and job order employees are not entitled to a personal computer. However, the aforementioned employees may be assigned the same that is allotted to existing plantilla positions which are currently vacated or unfilled.
5. All obsolete and/or malfunctioned ICT resources shall be returned-to-store to the Property and Procurement Management Division (PPMD) in coordination with the ITMS-Information Services Division.
6. Only the ITMS or its authorized personnel shall install, modify or upgrade any hardware and/or software.
7. Users shall not be allowed to disable, defeat, circumvent, or install any security mechanism in any of the DOE system, network or resources.
8. Only the ITMS or its authorized personnel shall inspect, modify, repair or maintain any ICT equipment, system or facilities. Equipment or software that is under warranty may not be inspected or altered without written authority from ITMS.
9. Only the ITMS or its authorized personnel shall move or transfer ICT equipment from one location to another, except for mobile computers.

10. The ITMS or its authorized personnel shall have the responsibility to maintain security of Internet resources against intrusion and destruction. They shall maintain a high degree of reliability and security of the systems.

Section VII. VIRUS PREVENTION

1. Only the ITMS or its authorized personnel shall install anti-virus program/s in any DOE computer, whether stand-alone or networked.
2. The ITMS shall regularly update the anti-virus program located in the servers and shall periodically give advisories to all Users to keep them informed of the best practices to combat viruses.

Section VIII. EMAIL ACCOUNTS

1. The DOE shall grant email accounts as a privilege to its employees, subject to the following conditions:
 - a. The employee shall use the email services only for work-related functions and activities and is prohibited to use the same for any illegal, immoral, and unethical purposes.
 - b. The email disk or mailbox space per user shall be set by the ITMS and it shall be the responsibility of the ITMS to inform the employees on their email disk or mailbox space allocation;
 - c. It shall be the responsibility of the employee not to exceed his/her allocated email disk or mailbox space and his/her email files are properly organized and maintained;
 - d. The allowable file size for attachments for incoming and outgoing emails shall be set by the ITMS who shall be responsible in informing the employees on the corresponding adjustments on the email attachment capacity.
 - e. On a case-to-case basis and for justifiable reasons, employees may request to increase their allotted limits.
2. Use of email is covered by Section V: SYSTEM ACCESS REQUIREMENTS and Section XI. PROHIBITED ACTS AND USES OF THE ICT FACILITIES AND RESOURCES.
3. The ITMS shall ensure that all outgoing emails emanating from the DOE email system shall have the following disclaimer:

'The information in this electronic message is confidential and intended only for the addressee and recipient. If you are not the addressee indicated in this message; you may not use, copy, disseminate this message. In such case, please delete this

email and notify the sender by reply email. Opinions, conclusions and other information expressed in this message are not given or endorsed nor considered official document and is not attributable to DOE unless otherwise expressly indicated by an authorized representative of DOE.'

4. The ITMS shall be responsible in providing and monitoring the email privileges of the DOE employees.
5. A DOE employee may use non-DOE email system consistent with the duties and responsibilities of the employee and this Policy.
6. Upon separation, termination, or other circumstances deemed legal by the DOE, email privileges shall be immediately terminated and the disk files containing the email files of the employee shall be surrendered.

Section IX. OWNERSHIP AND PRIVACY

1. All ICT resources in DOE are owned by the Government. The DOE reserves the right to monitor and/or log all network-based activity. The employee shall be responsible for surrendering all passwords, files, and/or other required resources, if requested by proper authority.
2. DOE has the right to access, read, review, monitor, copy or disclose all messages, data or information archived in the DOE computer system to competent authority at any time without need of prior notice.
3. By logging-in to the DOE ICT facilities, the user agrees to the terms and conditions of this Policy.

Section X. USER RESPONSIBILITIES

1. It shall be the responsibility of the Users to be aware, have knowledge and comply with this Policy.
2. Users shall report to the ITMS any suspected violations or breaches of security on the use of DOE ICT facilities and resources. Users shall cooperate with the system administrators in the conduct of any investigation of any violations or breaches of security.
3. Users shall refrain from playing games, watching video/video clips, and social networking during working hours.

Section XI. PROHIBITED ACTS AND USES OF THE ICT FACILITIES AND RESOURCES

1. General Principles in Proper Use of ICT Resources.

Users shall access or use only those services and parts of the ICT facilities or resources that are consistent with his/her duties and

responsibilities. The ICT facilities or resources shall be used in accordance with its authorized purpose. The uses and acts discussed in the following paragraphs shall be considered violations in the use of the DOE ICT facilities or resources.

2. Uses Contrary to Laws shall be defined as follows:

- a. Use of DOE ICT resources for criminal and unlawful activities.
- b. Unauthorized use of Copyrighted material. Prohibited Acts include but are not limited to:
 - i. Copying, reproduction, dissemination, distribution, use, importation, removal, alteration, substitution, modification, storage, unloading, downloading, communication, publication or broadcasting of copyrighted material without permission from the Copyright owner. Uncopyrighted materials copied from or through the DOE ICT System should be properly attributed;
 - ii. Infringement of Intellectual Property rights belonging to others through the use of ICT resources; and
 - iii. Infringement of Intellectual Property rights through the use of unauthorized or "pirated" softwares, peripherals or devices that are used in conjunction with or attached to DOE ICT facilities and resources.
- c. Hacking and Profiteering Schemes. These include but are not limited to:
 - i. Use of DOE ICT facilities and resources for hacking other ICT communications /computer systems; and
 - ii. Use of DOE ICT facilities and resources in any profiteering schemes that intends to defraud other people.
- d. Use of DOE ICT facilities and resources that is contrary to existing laws, rules and regulations.

3. Uses for Personal Benefit, Business or Partisan Activities. These shall include but are not limited to:

- i. Use of the DOE ICT facilities and resources for commercial purposes, advertisement, personal profit;
- ii. Use of the DOE ICT facilities and resources for any partisan political activities. Use of DOE ICT facilities and resources for political lobbying, disseminating information

or gathering support or contributions for social, political or cause-oriented group, which are inconsistent with the activities of the Department; and

- iii. Use of DOE ICT facilities and resources for viewing/uploading/downloading of pornographic materials or any activity unrelated or inappropriate to the duties and responsibilities of the User.

4. Acts that Damage the Integrity, Reliability, Confidentiality and Efficiency of the ICT System. These shall include but are not limited to:

- a. Interconnection of server systems, running particular service(s) such as Active Directory, DNS and DHCP, to the DOE LAN system;
- b. Destruction, deletion, removal, modification, or installation of any DOE-owned computer equipment, peripheral, operating system, disk partition, software, database, or other component of the ICT System;
- c. Acts that attempt to crash, tie up, or deny any service on DOE 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 (e.g. 26 MB or more); sending data packets that serve to flood the network bandwidth;
- d. Concealment, deletion, or modification of data or records pertaining to access to the DOE 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 pretending as other users when accessing, sending, receiving, processing or storing through or on DOE ICT System;
- f. Attempts or actions that tend to disable, defeat or circumvent any security mechanism installed in any of the DOE system, network or resources; and
- g. Alternate ISP connection to the DOE's internal network shall not be permitted. Devices using independent dial-up, DSL or leased-line shall not be connected to DOE's LAN.

5. Acts that Encroach on the Rights of Other Users. These shall include but are not limited to:

- a. Sending unsolicited mail such as chain-letters, advertisements, jokes, trivia, announcements to non-official groups or activities, offers, inquiries, and the like (spamming);
 - b. Accessing, downloading, uploading, producing, disseminating, or displaying material that could be considered offensive, pornographic, racially abusive, culturally insensitive, or libelous in nature;
 - c. Sending messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of the DOE; and
 - 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 spyware to monitor activities of other users.
6. Acts which Violate Privacy shall be defined as follows:
- a. Spying or Snooping. These include but are not limited to:
 - i. Accessing, or attempting to gain access to information, archives or systems that are outside their approved area and level of access;
 - ii. Decrypting, attempting to decrypt, or enabling others to decrypt such information which are intentionally encrypted, password-protected, or secured; and
 - iii. Re-routing or capture of data transmitted over the ICT System.
 - b. Unauthorized Disclosure. These shall include but are not limited to:
 - i. Copying, modification, dissemination, or use of confidential information such as, client's data submitted to DOE based on policy of trust and confidentiality, proprietary data and information; research materials and other material or information that is not classified for public use;
 - ii. Searching, or providing copies of, or modifications to, files, programs, or passwords belonging to other users, without the expressed permission of the owners of the said files, programs or passwords; and
 - iii. Disclosure of private personal data without expressed permission from the concerned person/s.

7. Acts that Waste Resources. These shall include but are not limited to:

- a. Habitual non-work related use of ICT resources;
- b. Printing of non-work related documents, files, data, or programs; and
- c. Sending of unsolicited files or messages.

Section XII. TOLERATED USE

1. Some ICT use, though unofficial, shall be tolerated. They are considered privileges that may be revoked at any time. These shall include:
 - a. Limited use of email for personal communication;
 - b. Limited use of instant messaging applications; and
 - c. Limited use of computers to play compressed audio files or audio CDs.

Limited use is defined as reasonable period of time or quantity that will not affect the efficiency and effectiveness of the User with respect to his/her work responsibilities.

Section XIII. DISCIPLINARY ACTION

1. Violations

Improper use of DOE ICT facilities and resources as enumerated in Offenses and Equivalent Administrative Offenses found in Annex B shall be subject to penalties. The Bureau/Service/Office Director, upon the recommendation of the investigating body, shall suspend the Internet and network privileges of the offender.

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-DOE Personnel

Non-DOE personnel found guilty of violating any of the provisions set forth in this Policy shall be barred from entering any DOE premises. The employee who permitted or authorized the non-DOE personnel to use or access the DOE ICT resources or systems or networks shall

also be held liable for all the violations that the person may have committed.

4. Penalties

In addition to the filing of an Administrative case and sanctions which shall be in accordance with the Civil Service Commission Uniform Rules and Regulations on Administrative Cases against the violators, appropriate charges shall be filed in court if offenses are punishable under the E-Commerce Law (RA 8792) or any other applicable Philippine Laws.

Section XIV. ENFORCEMENT PROCEDURES

1. Implementing Body

The ITMS upon approval of the Secretary shall establish a Group that will implement and monitor this Policy. The Group shall likewise be responsible for the imposition of penalties as set forth in this Policy and shall include personnel from the ITMS, Human Resource Management Division, Legal Services and representative from the DOE-Employee Association.

2. Jurisdiction of the Implementing Body on Investigation

- a. Upon receipt of a written report or complaint of, violation or breach of security, the implementing body shall conduct an investigation on the matter. 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, email account and/or other computer-accessible storage media, or authorize the system 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; and
 - v. To recommend 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.
- b. The implementing body shall submit the results and recommendation to the Secretary for appropriate action.

3. Appropriate Action

If the implementing body has evidences that warrants violation/s or breaches of security on the use of DOE ICT facilities and resources, the Secretary or his/her authorized representative shall pursue appropriate actions as provided for in the Civil Service Commission Uniform Rules and Regulations on Administrative Cases.

4. Filing of Charges

In cases where there is evidence of serious misconduct or possible criminal activity, appropriate charges shall be filed by the Secretary or his/her authorized representative to the proper authorities. This, however, does not prohibit any aggrieved party or complainant from instituting the filing of charges with the appropriate authorities.

5. External Legal Processes

The DOE ICT systems and network does not exist in isolation from other communities and jurisdictions and their laws. In cases where, as a result of investigations, subpoena or lawsuits, the DOE may be required by law to provide information or record/s in electronic or other forms to competent authority, use of the DOE ICT facilities and resources is granted subject to existing Philippine laws, rules and regulations.

Section XV. WAIVER AND DISCLAIMER

1. Disclaimer

While the DOE shall take measures to provide reliable and professional services in its ICT systems and network, DOE shall not guarantee, nor shall provide any warranties as to the operating characteristics of its ICT resources and facilities to any of its users.

2. Waiver

DOE shall not be responsible for any loss or damage, whether direct or indirect, implied or otherwise, that may arise from the use of the DOE ICT facilities and resources by any person or entity.


SECTION XVI. SEVERABILITY

If any part of this Policy shall be declared unconstitutional or invalid by a court of competent jurisdiction, such decision shall not affect the validity of the remaining provisions of this Policy, or the Policy in its entirety.

Section XVII. EFFECTIVITY AND AMENDMENT

1. This Policy shall be effective upon the approval of the Secretary.
2. The Department shall amend or modify this Policy to maintain the applicability of the Policy. These amendments or modifications shall form part of the overall DOE ICT Acceptable Usage and Security Policy, and shall be considered binding on all users.

Approved this _____ day of _____ 2011, at Fort Bonifacio, Taguig City, Metro Manila.

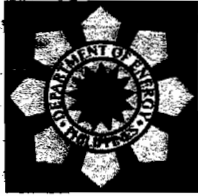

JOSE RENE D. ALMENDRAS
Secretary



IN REPLYING PLS CITE:
SDOE12-000014

JAN 12 2011





**Republic of the Philippines
Department of Energy (DOE)**

ICT ACCEPTABLE USAGE AND SECURITY POLICY

Annex A. DEFINITION OF TERMS

Access – To connect to the Internet; to “login”; to be in the Internet to browse, and 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.

Users - Refers to the following: (1) DOE personnel; (2) individuals connecting to DOE's public information service; or (3) other individuals authorized by DOE or its personnel to access and use the DOE ICT system, network or resources.

DOE Personnel – refers to current DOE officials and employees, including permanent, casual, contractual and co-terminous.

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).

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”, these viruses are best known for “spreading overnight from one to million computers 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.

Department of Energy “DOE” – Created under RA 7638 or the DOE Act of 1992

DOE System – This refers to the DOE Central Office and Field Offices ICT equipments, facilities, and information and communication systems.

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.

Hardware – Is defined as devices with which a computer is configured. Computers consist of processing units, memory, input/out units, etc.

Information and Communications Technology System/Resources/Facilities or ICT System/Resources/Facilities – Includes computers, terminals, printers, networks, modem banks, online and offline storage media, cellular phones, PABX System and related equipment, and software, databases and other data files that are owned, managed, or maintained by DOE. 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 Protocol (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.

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).

Local Area Network (LAN) – A network that connects computers in a small predetermined 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.

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.

Password – A secret word or phrase that one uses to gain admittance or access to information. It is a sequence of characters that one must input to gain access to a file, application, or computer system. Also called passkey.

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.

Router – A communication device between networks that determines the best path between them for optimal performance. Routers are used in complex 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); email services (email server).

Software – is a generic term for organized collections of computer data instructions, often broken into two major categories, namely:

- (i) system software - provides the basic non-task-specific functions of the computer and
- (ii) application software- it is used by users to accomplish specific task.

Spying - is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using illegal exploitation methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.

Snooping – is unauthorized access to another person's or company's data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

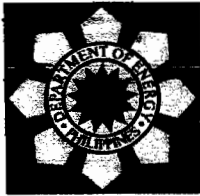
System and Network Administrator – Refers to the person designated to manage the particular system assigned to her/him, to oversee the day-to-day operation of the system, or to preliminarily determine who is permitted access to particular facilities and resources of the ICT System, whether hired on a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

Virus – (see Computer Virus)

Wireless Access Points - are specially configured nodes on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of WLAN radio signals.

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 ENERGY

ICT Acceptable Usage and Security Policy

Annex B. OFFENSES & EQUIVALENT ADMINISTRATIVE OFFENSES

ICT Resources Usage and Network Security Offenses	Equivalent Administrative Offense
1. Commercial Use – use of DOE ICT Resources for commercial purposes and product advertisement, for personal profit.	Simple Misconduct
2. Religious or Political Lobbying – use of DOE 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 DOE 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 DOE 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 DOE'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
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 email or private communications of other users, unless otherwise requested to do so by said users.	Simple Misconduct
16. Misrepresentation in sending email messages.	Simple Misconduct
17. Systems Software and Hardware Removal – unauthorized removal or modification of System software and hardware on any DOE-ICT Resource.	Simple Misconduct
18. Damaging/Vandalizing – damaging or vandalizing any of the Department's ICT Resource including but not limited to all facilities, equipment, computer files, hardware and software.	Simple Misconduct
19. Unauthorized manipulation/changing of DOE ICT	Simple Misconduct

Network architecture or setup.	
20. Software and Hardware Installation – unauthorized installation of software and hardware on any of the DOE 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. 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
23. Changing of IP Address and Network configuration without the approval of the ITMS.	Violation of Reasonable Rules and Regulations
24. Recreational Use – no ICT resource must be used for playing computer game, whether individually or in a multiplayer setting or to be used in watching movies during working hours.	Violation of Reasonable Rules and Regulations
25. Tolerating or not reporting co-employees who use ICT resources for recreational purposes as mentioned in item no. 24.	Violation of Reasonable Rules and Regulations

OFFENSES & PENALTIES

OFFENSE	PENALTIES
Simple Misconduct	1 st Offense – Reprimand; 2 nd Offense – Suspension for one (1) month and one (1) day to six (6) months; 3 rd 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