

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 consists 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 PSHS 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 PSHS Network responsible for operating the resource.

Bandwidth – The number of bits of information that can be 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.

PSHS System – This refers to PSHS 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 PSHS. 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 in 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-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.

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 him/her, 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 do design engineers, architects, graphic designers and any organization, department, use those or individual that requires a faster microprocessor, larger amount of random access memory (RAM), and special features such as high-speed graphics adapters.

COMPUTER SCIENCE/ TECHNOLOGY LABORATORY RULES AND REGULATIONS

1. There shall be no smoking, drinking or eating in the computer laboratories.
2. Loitering is strictly prohibited within the laboratory.
3. Bags and large containers shall not be allowed in the work area.
4. Inserting foreign objects into any equipment in the laboratory shall be considered vandalism and shall be penalized in accordance with the PSHS Code of Conduct. Pending the investigation, suspension of laboratory privileges shall be imposed as follows:
 - 1st offense: 1 week suspension of laboratory privileges
 - 2nd offense: 2 weeks suspension of laboratory privileges
 - 3rd offense: 1 month suspension of laboratory privileges
5. Defacing laboratory equipment or furniture shall likewise be considered as vandalism and dealt with as outlined above.
6. Any modification introduced to existing hardware configuration of the computers without permission from the laboratory technician and laboratory instructor is prohibited.
7. Any permanent modification to the existing software configurations installed in the computers is likewise strictly prohibited.
8. Unauthorized access to user files (i.e. hacking into another user's workplace), copying of laboratory activities/machine and exercises/machine problems from other students, and the like, shall be considered cheating and shall be dealt with in accordance with the PSHS Code of Conduct. Hacking shall also be subject to applicable Philippine Laws on Copyright.
9. Roaming around the room is discouraged. Punishment shall be at the discretion of the instructor.
10. Playing computer games and other non-academic hardware or software is not allowed.
11. Leave the laboratory neat after every class:
 - a. place the keyboard and mouse on top of the CPU tower,
 - b. check the room for trash and personal items, and
 - c. put the chairs in order before leaving the room.