



Republika ng Pilipinas
KAGAWARAN NG KAGALINGANG PANLIPUNANAT PAGPAPAUNLAD
(DEPARTMENT OF SOCIAL WELFARE AND DEVELOPMENT)
BATASAN PAMBANSA COMPLEX, CONSTITUTION HILLS
QUEZON CITY



DEPT. OF SOCIAL WELFARE & DEVT.
IBP ROAD, CONSTITUTION HILLS, Q.C.

Memorandum Circular No. 26
Series of 2004

JUN 8 1174

LEGAL SERVICE
RECEIVED BY: me

Subject: Information Technology (IT) Usage and Network Security Policy

I. RATIONALE

Information plays a vital role in enabling the Department of Social Welfare and Development to effectively carry out its steering and rowing functions. Accordingly, sound information and knowledge management are imperative to ensure that security and protection are accorded to this information commensurate with their value to the organization.

The recognition of the importance of Information Technology and the organizational impact of computer-based information systems in realizing the DSWD's mission and vision require corresponding adjustments in operational processes, work flows and ethical/behavioral dimensions. Thus, in tandem with laws and other statutes, a renewal of existing policies and guidelines relative to IT utilization is needed.

II. LEGAL BASES

1. Republic Act No. 8792 (Electronic Commerce Act) - 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.
2. Republic Act No. 8293 (Intellectual Property Code) - An Act Prescribing the Intellectual Property Code and Establishing the Intellectual Property Office, Providing for its Powers and Functions, and for Other Purposes.
3. Republic Act No. 9239 (Optical Media Act) - An Act Regulating Optical Media, Reorganizing for this Purpose the Videogram Regulatory Board, Providing Penalties Thereof, and for Other Purposes.
4. Republic Act No. 6713 (Code of Conduct and Ethical Standards for Public Officials and Employees) - An Act Establishing a Code of Conduct and Ethical Standards for Public Officials and Employees, To Uphold the Time-Honored Principle of Public Office Being a Public Trust, Granting Incentives and Rewards for Exemplary Service, Enumerating Prohibited Acts and Transactions and Providing Penalties for Violations Thereof and for Other Purposes.
5. Malacanang Memorandum Circular No. 115 - Directing All Departments and Agencies and Instrumentalities to Legalize Their Computer Software
6. Executive Order 265 - Approving and Adopting the Government Information Systems Plan (GISP) as Framework and Guide for all Computerization Efforts in Government.

7. Administrative Order 332 (RPWeb) - Directing all government agencies and instrumentalities including local government units to undertake electronic interconnection through the Internet to be known as the RPWEB.
8. National Computer Center (NCC) Memorandum Circular 2003-01 - Guidelines on Compliance to the E-Commerce Act (R.A. 8792) and Stage Two and Three of the UN-ASPA Five Stages of E-Government.
9. NCC Memorandum Circular 2002-01 - Guidelines on Creation of the Agency's Official Website and Compliance to E-Commerce Law and Stage One of the UN-ASPA Stages of E-Government.
10. NCC Memorandum Circular 2000-01 - Prescribing Guidelines for Planning and Managing the Agency's I.T. Infrastructure for Connection to Government Information Infrastructure Through RP-Web.
11. DSWD Administrative Order No. 14 (Series of 2004) - Guidelines on the Adoption of Progressive Disciplining in the DSWD.
12. DSWD Memorandum Order No. 30 (Series of 2003) - Constituting the Management Information System Service of DSWD.
13. DSWD Memorandum Circular No. 22 (Series of 2003) - Implementing Rule on the Rationalization, Acquisition, Use and Maintenance of Information and Communication Technology (ICT) Devices.
14. DSWD Administrative Order 192 (Series of 2002) - Guidance on the Proper Use and Maintenance of Equipment.
15. DSWD Department Order No. 6 (Series of 1998) - Management Information System Guidelines.
16. DSWD Department Order No. 3 (Series of 1997) - Computer Software Standardization and Legalization Guidelines.
17. Commission on Audit Circular No. 97-003 - Accounting Guidelines on the Acquisition, Maintenance and Disposition of Information Technology Resources.

III. SCOPE OF THE POLICY

As a productivity tool, the use of IT, just like any office equipment and machinery, is a privilege extended in good faith by the government through the DSWD. Hence, all users are directed to use these facilities and resources responsibly to preserve their security, integrity, and availability as well as assure the authentication and accountability of each user.

In this regard, this policy guideline is issued to define the acceptable mode of IT usage. Unless otherwise expressly stated, this guideline shall be applicable to:

1. Users Covered. This policy applies to all personnel employed or contracted by DSWD, its agencies and offices, including its trainees.
2. Components Covered. This policy covers the proper use of the IT facilities and resources of the DSWD, which include all IT equipment, software, accessories, networking facilities and services, and most importantly, the resulting data and information generated from it.

IV. 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 hardware, software, services, and new perspectives in the use of IT resources.

V. GENERAL IT USAGE POLICY

1. Use of IT Resources. Agency IT resources are to be used for work-related activities and functions. This is to ensure the effective use of IT resources and shall equally apply to all users as defined in Chapter III section 1.
 - a. User Responsibilities. A user may access only those services and parts of the IT System that are consistent with his/her duties and responsibilities. The IT System should be used in accordance with its authorized purpose.
 - i. Logging. All users shall log in using their own usernames and passwords. The Agency reserves the right to hold the employee liable for damages caused by his/her failure to protect the confidentiality of his/her password in accordance with the above guidelines.
 - ii. Reporting of Problems / User Cooperation. Users are enjoined to cooperate by reporting suspected abuse, especially any damage to, or problems with their files, workstations or other IT equipment to their immediate supervisor or Head of the Office, Bureau, Service or Unit (HOBSU). If there be technical problems that cannot be resolved at the OBSU level, this must be reported to the MISS, OBSU IT designated staff, or the IT designated staff for each Field Office (FO) so that appropriate action can be taken.
 - iii. Turnovers. The employee is obligated to surrender all passwords, files, and/or other required resources when he/she is resigning, going on a long leave of absence, or terminated in the presence of his/her direct supervisor.
 - iv. Implied User Agreement to Terms and Conditions. By logging-in to the DSWD IT facilities, the user agrees to the terms and conditions of this Policy.
 - b. Tolerated Use. Some IT use, though unofficial, may be tolerated. These are considered privileges that may be revoked at any time. They include:
 - i. The use of email for personal communication.
 - ii. The use of instant messaging applications.

The DSWD 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 on all users.
 - c. Exception. The Agency Head may approve the use of IT resources beyond the scope of this policy under the following conditions:
 - i. The intended use of IT resources serves a legitimate Agency interest.
 - ii. The intended use of IT resources is for educational purposes related to the employee's job function.

2. Computer System Components

a. Hardware

- i. Standards. Procurement of PC's shall be based on their intended use as evaluated by MISS or FO IT designated staff. Multimedia devices, sound cards, video cards and other peripherals shall be strictly rationalized. Annex B enumerates current hardware standards which will be updated from time to time based on commercially available standards.
- ii. Maintenance. Management Information System Service (MISS) personnel, OBSU IT designated staff, and the FO IT designated staff are the only authorized entities who may inspect and/or provide technical support services to all IT Resources/Equipment.
- iii. Allocation. Based on available Agency resources, allocation of PC's shall be rationalized with the aim of achieving a 1:1 pc-user ratio for technical staff and 1:2 ratio for clerical/support staff.
- iv. Physical Transfer of Hardware. MISS or FO IT designated staff shall be informed of any physical transfer of hardware from one office to another so that appropriate settings and configurations can be performed.

b. Software

- i. Authorized Software. Only the software enumerated in the List of Authorized Software found in Annex C shall be installed and used in DSWD computers. This list may be updated from time to time to reflect new software required by DSWD. Software not included in the list but is used by a particular OBSU may be added once approved for usage, as recommended by the MISS to DSWD Management.
- ii. Software Licenses. All commercial software used in the Department should have licenses. Use of unlicensed software is an act punishable by law under the E-Commerce Act (Sec. 33b) and the Intellectual Property Code (Sec. 217).
- iii. License Management. The MISS and FO IT designated staff shall be the main custodian of all Paper and Original Equipment Manufacturer (OEM) Licenses and Installation Disks for the Central Office and Field Offices respectively.
- iv. Installation and Upgrade. MISS personnel / FO IT designated staff are the only authorized entities who may install and upgrade software.
- v. Systems Inspection and Deletions. The MISS / FO IT designated staff may delete files or software that are unauthorized, provided that prior to this deletion or modification, consultation is done with the head of office. Deletion and modification should be done in the presence of the user or his immediate supervisor.
- vi. Desktop Settings. Users should not use personal, political, or religious pictures as their desktop wallpaper. Desktop themes should not also be installed since this usually use up computer memory resulting in a slower processing time. MISS will provide a standard desktop wallpaper containing the Department's logo and tagline for all computers to achieve a corporate identity for the Department.

3. Network Components.

- a. Network Connections. MISS personnel / FO IT designated staff are the only authorized entities who may install, remove, or modify network connections. Unauthorized personnel may not alter physical network connections.
- b. Network Settings. MISS personnel / FO IT designated staff are the only authorized entities who may alter network settings. The Internet Protocol (IP) address assigned to one computer may not be used in other computers.
- c. Network Monitoring. The Agency reserves the right to monitor and/or log all network-based activity.

4. Security Requirements

- a. Access Privilege. All qualified users of the DSWD IT facilities shall be issued a unique login name and password to gain access to network resources.
- b. Passwords.
 - i. Confidentiality. It is the responsibility of the user to ensure that his/her password remains secret. He/she should 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.
 - ii. Standards. Passwords are to be a minimum of six (6) alphanumeric characters. Passwords should not consist of common words or variations on the user's name, login name, server name, or agency name. Passwords could be a combination of names and/or dates that only the user understands.
 - iii. Maintenance. Users should change their passwords quarterly to ensure utmost security.
- c. Username. The standard naming convention used for usernames shall be the first letter of the user's first name, his/her middle initial, and his/her last name.

5. Internet Connections and Email Accounts

- a. Internet Browser Settings. The default homepage of all Internet browsers should be the DSWD website (<http://www.dswd.gov.ph>)
- b. Internet Access. Internet access shall be rationalized primarily based on the actual job functions, frequency of use, volume of work requirements of each office, and limited by available Internet resources. Offices, Services, Bureaus and Units (OSBUs) must submit a written request if they need additional Internet connections. If there are still available Internet resources, requests shall be reviewed by the MISS for approval.

- c. DSWD E-mail Privileges. DSWD through the MISS shall grant email accounts to all HOBSU's and key technical staff (limited only by the network's bandwidth), subject to the following conditions:
 - i. Responsibility of Maintenance/Usage.
 1. The employee may not use e-mail for purposes that are illegal, inappropriate, or disallowed by the DSWD. Examples of these can be found in Annex D.
 2. Official communication intended to be transmitted through email should be approved by the Heads of Offices, Bureaus, Services, or Units (HOBSU's) or by the appropriate Officer-In-Charge before it is sent.
 3. The email disk space per user is limited to 10 MB. It is the responsibility of the user to maintain his email files, i.e. to delete unwanted files, and to save those that are required for archiving.
 4. Attachments to mails should be limited to 1 MB per message.
 - ii. Other Email Accounts. The user may use non-DSWD email services, provided the use of these mail services are consistent with the duties and responsibilities of the employee.
 - iii. Surrender and Waiver. It is understood that email privileges including the disk files containing the email files of the user are surrendered upon separation, termination, or other circumstances deemed legal by the DSWD.

VI. VIRUS PREVENTION

1. Authorized Anti-virus Program. No anti-virus programs are allowed to be installed in any DSWD computer, whether stand-alone or networked, except those prescribed by the MISS.
2. Installation. MISS personnel / FO IT designated staff is the authorized entity to install Anti-virus software.
3. Announcements and Updates. The MISS is responsible for the daily updating of the anti-virus program located in the servers. The MISS shall periodically give advisories to all users to keep them informed of the best practices to combat viruses and warnings regarding newly discovered viruses.
4. User Responsibility in Anti-Virus Protection. It is the responsibility of the user to periodically update their anti-virus software and scan his/her files regularly for viruses. This includes files saved in removable storage devices (e.g. diskettes, cd-roms, etc.), files downloaded from the Internet and files attached to emails.

VII. PROHIBITED USAGE AND DISCIPLINARY ACTIONS

1. Prohibited Use. The following uses and acts, discussed thoroughly in Annex E, are considered violations in the use of the DSWD IT facilities and network:
 - a. Uses contrary to laws, customs, mores and ethical behavior.
 - b. Uses for personal benefit, business, or partisan activities.
 - c. Acts that damage the integrity, reliability, confidentiality and efficiency of the IT system.

- d. Acts that encroach on the rights of other users.
- e. Acts which violate privacy.

2. Disciplinary Action.

- a. Violations. Improper use of IT resources is subject to penalties. The Agency Head may, upon the recommendation of an investigative body, put a preventive suspension to the Internet, network and the IT resource/facility usage privileges of the offender/suspected violator.
- b. Applicable Laws. All disciplinary action proceedings shall follow the Civil Service Commission Uniform Rules and Regulations on Administrative cases, DSWD Administrative Order 14 (Guidelines on the Adoption of Progressive Disciplining in the DSWD) and/or legal action provided by applicable Philippine laws e.g. E-Commerce Act and Intellectual Property Code.
- c. Penalties for non-DSWD Personnel. Any non-DSWD personnel found guilty of violating any of the provisions set forth in this Policy, will be barred from entering any DSWD premises. The employee who gave permission to the visitor to access the DSWD network will also be held liable for all the violations that the visitor may commit.
- d. 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 Electronic Commerce Act, Intellectual Property Code or any other applicable Philippine law, when deemed appropriate.

VIII. ENFORCEMENT PROCEDURES

The MISS and the IT designated staff are designated to implement this Policy and monitor violations in the DSWD Central Office and the regional offices, respectively. They will immediately inform the Head of Office where the violation occurred. If they document repeated violations by persons or groups and after repeated warnings, they will file the necessary complaint following the normal procedure for administrative cases. A complaint filed should point out specific violations to this Policy.

In cases where there is evidence of serious misconduct or possible criminal activity, appropriate charges shall be filed by the Agency Head to 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.

The DSWD 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, DSWD 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.

IX. WAIVER AND DISCLAIMER

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

X. EFFECTIVITY

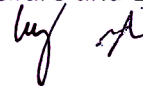
This Memorandum Circular shall take effect immediately and amends previous orders inconsistent herewith.



CORAZON JULIANO-SOLIMAN

Secretary

Department of Social Welfare and Development



A CERTIFIED COPY: 11



CARMELITA E. ZAFRA
Chief, General Services Division
and OIC, Records Unit

Annex A Definition of Terms

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 Social Welfare and Development; or any of its offices or institutions.

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

Bandwidth – this is the range of signal frequencies that can be carried on a communication channel. It is measured in cycles per second, or hertz (HZ) between the highest and lowest frequencies. This is more commonly expressed as bits per second (bps).

Email – a means or system for transmitting messages electronically (as between computers on a network); messages sent and received electronically through an e-mail system.

Hacking – to gain access to a computer illegally.

Hardware – the electronic and physical components, boards, peripherals and equipment that make up a computer system as distinguished from the programs (software) that tell these components what to do. It is the physical component that consists of input devices, central processor, output devices and storage devices.

Information Technology System (IT System) – includes computers, terminals, printers, networks, modem

banks, online and offline storage media and related equipment, and software, databases and other data files that are owned, managed, or maintained by DSWD. 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 IT System.

Internet- an electronic communications network that connects computer networks and organizational computer facilities around the world

IP Address – An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.

Multimedia – the use of computers to present text, graphics, video, animation, and sound in an integrated way.

Network – A group of two or more computer systems linked together. There are many types of computer networks, including:

Local Area Network (LAN) – a computer network limited to the immediate area, usually the same building or floor of a building.

Wide Area Network (WAN) – a computer network that is meant to cover a wide geographic area, usually over telephone lines.

Operating System – software that supervises and controls tasks on a computer. It directs a computer's operations, by controlling and scheduling the execution of other programs and managing storage and input/output processes.

Server – A computer or device on a network that manages network resources. For example, a *file server* is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A *print server* is a computer that manages one or more printers, and a *network server* is a computer that manages network traffic. A database *server* is a computer system that processes database queries.

Software – a set of instructions to a computer to execute a command or process data. It is the non-physical component of a computer, which maybe an operating system, a development language, database management system, computer tools and utilities, or an application package, as well as the machine coded instructions that direct and control different hardware facilities.

User ID – Also known as a username; it is an identifier, or a handle, for a user on the Internet or Network.

Users –Refers to one or more of the following: (1) current employees of

DSWD either permanent, casual or contractual; or (2) individuals connecting to a public information service. In addition, a user must be specifically authorized to use a particular IT resource by DSWD.

Virus –A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Some people distinguish between general viruses and *worms*. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

Workstation – a computer intended for professional or business use, and is faster and more capable than a personal computer.



Annex C
List of Authorized Software

1. Operating System	Windows 95/98/2000/XP
2. Office Productivity Tool	MS Office 97/2000 / XP
3. Anti-Virus	McAfee Virus Scan 4.x or higher
4. Network Operating System	Linux and Windows NT/2000 Server
5. Mail Server	MS Exchange 2000
6. Firewall	MS ISA 2000
7. Database Server	MS SQL Server 2000
8. Web Browser	Internet Explorer 5.x or higher
9. Development Tool	MS Visual Studio 6.0
10. Statistical Package	SPSS
11. Utilities	Acrobat Distiller Acrobat Reader WinZip
12. Graphic Tools	Adobe Photoshop

Annex D
Examples of Inappropriate Email Use

1. Chain Mail – email sent repeatedly from user to user, with requests to send to others.
2. Harassing or hate mail – any threatening or abusive email sent to individuals or organizations which violates DSWD policies or rules.
3. Viruses – malicious computer codes that include, but are not limited to, computer virus, Trojan Horse, worm, and hoax.
4. Spam or email bombing attacks – intentional email transmissions that disrupt normal email service
5. Junk mail – unsolicited email that is not related to DSWD business and is sent without a reasonable expectation that the recipient would be welcome receiving it.
6. False identification – any actions that defraud another or misrepresent or fail to accurately identify the sender.

Annex E
PROHIBITED ACTS AND USES OF THE IT RESOURCES

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

- a. Criminal Use. Users should not use the DSWD Network Information resources for criminal activities.
- b. 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. Users should properly attribute any material they copy from or through the IT System.
 - 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.

2. Uses for Personal Benefit, Business or Partisan Activities

- a. Commercial Use. Use of the IT 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 IT System for any partisan political activities. Use of IT 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.
- c. Games and Entertainment. Use of IT resources to play games, watch video, or any activity unrelated or inappropriate to the duties and responsibilities of the user.

3. Acts that Damage the Integrity, Reliability, Confidentiality and Efficiency of the IT System.

- a. Unauthorized deletion, removal, modification, installation and/or destruction of any computer equipment, peripheral, operating system, disk partition, software, database, or other component of the IT System;
- b. Connection of any computer unit or external network to the IT System without the permission of the MISS or the Agency Head.
- c. Acts that attempt to crash, tie up, or deny any service on the IT 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 IT 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 IT System.

4. Acts that Encroach on the Rights of Other Users.

- a. Sending Unsolicited Email. 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 DSWD.
- 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.

5. 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 IT System.
 - iv. Accessing, or attempting to access, restricted portions of the system, such as email 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; DSWD 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 IT 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.

6. 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.
- d. Using Internet resources not related to work (e.g. browsing multiple websites at one time, downloading unnecessary files).

Annex F
Offenses and Equivalent Administrative Offenses

IT Usage and Network Security Policy	Equivalent Administrative Offense	Comments of the Civil Service Commission
1. Commercial Use – Use of DSWD IT Resources for commercial purposes, and product advertisement, for personal profit.	Dishonesty or Grave Misconduct	The said offense may constitute Grave Misconduct but as to Dishonesty there must be at least a showing of concealment or distortion of the truth.
2. Religious or Political Lobbying – Use of DSWD IT 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 DSWD IT 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	The same offense may also be punished under Grave Misconduct or Conduct Prejudicial to the Best Interest of the Service.
4. Criminal Use – using the resources for criminal activities.	Grave Misconduct	The corresponding administrative offense is appropriate. It may also be punished under Conduct Prejudicial to the Best Interest of the Service.
5. Wiretapping and Traffic Capture – the unauthorized rerouting or capture of traffic transmitted over the voice or data network.	Grave Misconduct	The corresponding administrative offense if appropriate.
6. Stealing – Stealing of information resources both hardware or software or any part of the network resource.	Grave Misconduct	The corresponding administrative offense is appropriate, or may be punished under Conduct Prejudicial to the Best Interest of the Service.
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 IT resources.	Grave Misconduct	The offense may also constitute Dishonesty.
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	The corresponding administrative offense is appropriate.
9. Intrusion – attempts to disable, defeat or circumvent any DSWD network security settings. Unauthorized access to another computer or network thru decrypting, hacking, hijacking, spoofing, etc.	Grave Misconduct	The corresponding administrative offense is appropriate.
10. Access of other accounts or files within or outside DSWD's computers and communication facilities without proper authorization.	Simple Misconduct	The corresponding administrative offense is appropriate.
11. Copying, renaming or changing		



information on files/programs that belong to another user, unless permission was given by the said user	Simple Misconduct	The corresponding administrative offense is appropriate.
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	The acts committed may also constitute Sexual Harassment, Grave Misconduct and Oppression depending on the acts actually committed.
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	The acts committed may also constitute Sexual Harassment, Grave Misconduct and Oppression depending on the acts actually committed and the circumstances of the offender and the offended party.
14. Prohibitive Materials – Using or encouraging the use of materials that includes instructions to gain unauthorized access (e.g. Hacker's Guide)	Simple Misconduct	Violation of Reasonable Office Rules and Regulations is more appropriate for this offense.
15. Unauthorized reading of email or private communications of other users, unless otherwise requested to do so by said users.	Simple Misconduct	The corresponding administrative offense is appropriate.
16. Misrepresentation in sending email messages.	Simple Misconduct	Depending on the acts and circumstances of the offense committed, the same may also constitute as Violation of Reasonable Office Rules and Regulations.
17. Systems Software and Hardware Removal – Unauthorized removal or modification of System software and hardware on any of the DSWD IT facilities.	Simple Misconduct	The corresponding administrative offense is appropriate.
18. Damaging/Vandalizing – Damaging or vandalizing any of the Department's IT resources including but not limited to all facilities, equipment, computer files, hardware and software.	Simple Misconduct	The same may be appreciated as grave misconduct depending on the gravity of the offense.
19. Unauthorized manipulation/changing of the DSWD Network architecture or setup.	Simple Misconduct	The corresponding administrative offense is appropriate.
20. Software and Hardware Installation – Unauthorized installation of software and hardware on any of the DSWD IT resources.	Violation of Reasonable Rules and Regulations	The corresponding administrative offense is appropriate.
21. Not cooperating with any investigative process in line with computer, network or system abuse.	Violation of Reasonable Rules and Regulations	The corresponding administrative offense is appropriate.
22. Disclosure of DSWD Confidential Information	Disclosing or misusing confidential or classified information officially known to him by reason of his office and not available to	The corresponding administrative offense is appropriate.

	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	Depending on the acts committed, the said offense may also constitute Sexual Harassment.
24. Changing of IP Address and Network configuration without the approval of MISS	Violation of Reasonable Rules and Regulations	The corresponding administrative offense is appropriate.
25. Recreational Use – No IT 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	The corresponding administrative offense is appropriate.
26. Tolerating or not reporting co-employees who use IT resources for recreational purposes as mentioned in item no. 25.	Violation of Reasonable Rules and Regulations	The corresponding administrative offense is appropriate.

*Adapted from DOST Administrative Order No. 12 (Series of 2003) – DOST ICT Usage and Security Policy