Republic of the Philippines
Department of Social Welfare and Development
IBP Road, Batasan Pambansa Complex, Constitution Hills, Quezon City 1126
Telephone Nos. (632) 931-8101 to 07; Telefax (632) 931-8191
E-mail: osec@dswd.gov.ph
Website: http://www.dswd.gov.ph

ADMINISTRATIVE ORDER NO. 09
Series of 2015

SUBJECT:
POLICY ON STEWARDSHIP, ACCEPTABLE USE AND SECURITY OF DSWD INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) RESOURCES

I. RATIONALE

Computers and networks are powerful Information and Communication Technologies (ICT) for accessing and distributing information and knowledge. Information and Communication Technologies are provided for Department of Social Welfare and Development Officers and Staff as productivity tools and services for mission related functions and activities. Appropriate rules and regulations must be enforced to ensure equitable, secure and reliable access to these resources.

II. LEGAL BASES

A. 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 Thereon and for Other Purposes

B. Republic Act No. 8293 (Intellectual Property) - An Act Prescribing the Intellectual Property Code and Establishing the Intellectual Property Office, Providing for its Powers and Functions and for Other Purposes

C. Republic Act No. 9239 (Optical Media Act) - An Act Regulating Optical Media, Reorganizing for this Purpose the Ideogram Regulatory Board, Providing Penalties Thereof and for Other Purposes

D. Republic Act No. 6713 (Code of Conduct and Ethical Standards for Public Officials and Employees) - An Act Establishing a Code of Conduct and Ethnical 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

E. Republic Act No. 10175 (Cyber Crime Prevention Act) - An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes

F. Republic Act No. 10173 (Data Privacy Act) - An Act Protecting Individual Personal Information in Information and Communications Systems in The Government and the Private Sector, Creating for this Purpose a National Privacy Commission and for Other Purposes

G. Malacañan Memorandum Circular No.115 - Directing All Departments and Agencies and Instrumentalities to Legalize Their Computer Software

H. DSWD Administrative Order No. 14 (Series of 2004) - Guidelines on the Adoption of Progressive Disciplining in the DSWD

I. DSWD Memorandum Order No. 30 (Series of 2003) - Constituting the Management Information System Service of DSWD

J. DSWD Memorandum Circular No. 22 (Series of 2003) - Implementing Rules on the Rationalization, Acquisition, Use and Maintenance of Information and Communication Technology (ICT) Devices

K. DSWD Administrative Order 192 (Series of 2002) - Guidance on the Proper Use and Maintenance of Equipment

L. DSWD Department Order No. 3 (Series of 1997) - Computer Software Standardization and Legalization Guidelines

M. Commission on Audit Circular No. 97-003 - Accounting Guidelines on the Acquisition, Maintenance and Disposition of Information-Communications Technology Resources

III. OBJECTIVES

The following regulations will govern the use of ICT resources of DSWD. These regulations aim to:

A. Build an ICT infrastructure that promotes the mission and vision of DSWD;

B. Protect the integrity, accessibility and confidentiality of the ICT resources of DSWD;

C. Maintain and enhance the availability and efficiency of the ICT resources of DSWD;

D. Establish processes for addressing policy violations and providing sanctions for violators;

E. Warn users that the use of ICT resources for any unauthorized purposes is prohibited, and meting of censure or punishments for established violations; and,

F. Update existing policies attuned to current business requirements.

IV. DEFINITION OF TERMS

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

V. COVERAGE

This policy applies to all employees employed or contracted by DSWD Central Office and its Field Offices whether regular/permanent, casual, contractual or MOA, including trainees.

The Human Resource Development Bureau (HRDB), in coordination with the IMB, shall include this policy in their awareness and compliance campaigns for all employees and other related fora.

VI. ICT ACCEPTABLE USE POLICY

A. Use of ICT Resources

The Department's use of ICT resources must be limited to work-related activities and functions and to authorized work-designated activities.

B. User Responsibilities

A user may only access 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.

C. Reporting of Problems and User Cooperation

ICT Users are enjoined to cooperate by reporting suspected abuse, especially any damage to, or problems with their files, workstations or other ICT equipment to the ICTMS Service Desk.

Users are responsible for the daily operational upkeep and maintenance of their ICT equipment. If there are technical problems that cannot be resolved by the user, this must be reported to the IMB Service Desk, deputized ICT staff of existing Project Management Offices or the Regional Information and Communication Technology Management Unit (RICTMU) for each FO using the IMB sanctioned service support process so that appropriate action can be taken.

D. Turnovers

The employee is obligated to surrender to the designated OBSU ICT focal person and in the presence of his/her direct supervisor all passwords, files, and/or other required resources upon resignation, leave of absence of more than 15 days, retirement, transfer within or outside the agency due to promotion, reassignment, detail or secondment, or upon termination. A clearance from the IMB/RICTMU shall be issued to ascertain the termination of his/her access privileges to the ICT system.

VII. Stewardship of ICT Resources

This policy covers the acceptable use of the ICT resources of the DSWD, which include all computing hardware, software, network facilities and services, and the concomitant data, information and knowledge they produce.

A. Computing Hardware

1. Computing Standards

Procurement of computing equipment shall be based on their intended use and service objective as evaluated by the IMB or RICTMU. Annex B enumerates current minimum hardware standards, which will be updated on a quarterly basis based on prevailing industry standards and specified service objectives.

2. Maintenance

IMB personnel, RICTMU and DSWD sanctioned service provider with Active Service Level Agreements (SLAs) are the only entities who are authorized to inspect and/or provide technical support services to all ICT Resources/Equipment.

3. Allocation

Based on available DSWD resources, allocation of computing equipment shall be rationalized. The aim of achieving a 1:1 Computer to User ratio will be pursued through the following implementation models:

a) Desktop Computing for Office Productivity;

b) Workstation Computing for Specialized Applications;

c) Mobile Computing for Office Productivity; and,

d) Physical Transfer of Hardware.

The Property Management Division (PMD) of the Administrative Service and their regional counterparts shall coordinate with the IMB or RICTMUs,

with regard to any physical transfer of hardware from one office to another so that appropriate settings and configurations can be performed. This should be accompanied by PMD-sanctioned documentation.

B. Software

1. Authorized Software

Only the software enumerated in the List of Authorized Software found in Annex C shall be installed and used in all 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 required by a particular OBSU may be added with appropriate justification for usage, as recommended by the IMB.

2. Software Licenses

All proprietary software used in the Department should have the appropriate licenses. Use of unlicensed software is an act punishable by law under the Section 33b of the E-Commerce Act and under Section 217 of the Intellectual Property Code.

3. Software License Management

The IMB and FO RICTMUs shall be the main custodian of all Central Office licenses in any format and of ancillary Installation Disks for the Field Offices. All licenses must be kept inside a secure facility.

4. Software Installation and Upgrade

IMB personnel, FO RICTMU personnel and ICTMS-sanctioned service providers are the entities who are authorized to install and upgrade computing software.

5. Software Inspection and Deletions

The IMB/RICTMU may delete files or software that are unauthorized, provided that consultation with the head of office was done prior to the deletion or modification.

The IMB/RICTMU shall conduct periodic inspection of all DSWD Computers and may consequently delete files or software that are unauthorized.

Deletion and modification of an unauthorized file or software should be done with the knowledge and in the presence of the user or his/her immediate supervisor.

C. Security

1. Host Administrator/Root Accounts

For a higher level of security and service support, IMB personnel and RICTMU staff are the only entities who are authorized to have access to Host Administrator/Root Accounts for all computing equipment.

2. User Accounts

Each user shall be provided with their individual user accounts. The standard naming convention used for usernames shall be as follows:

> First letter of the user's first name, followed by the user's middle initial and then the user's last name
>
> *e.g. If user's full name is Juan G. Gonzales, his username shall be JGGonzales*

3. Passwords

a) *Confidentiality*

It is the responsibility of the user to ensure that his/her password remains secret. The user should not share it with other individuals. The exception is when an employee surrenders his/her password as required in this policy. In cases of information system applications, supervisors or authorized focal persons may have override access accounts that can access subordinate accounts for business continuity.

b) *Standards*

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

c) *Maintenance*

Users should change their passwords at least every month to ensure optimum security.

4. Host Computer Desktop Settings

Users should not use personal, political, or religious pictures as their desktop wallpapers and screensavers. ICTMS will provide standard desktop wallpaper for all computers to achieve an enterprise identity for the Department.

5. Authorized Security Software

No security programs are allowed to be installed in any DSWD computer, whether stand-alone or networked, except those prescribed by the IMB.

6. Installation

IMB personnel and RICTMU staff are the entities authorized to install security software.

7. Announcements and Updates

The IMB shall periodically give advisories to all users via IMB email advisories to keep them informed of the best practices to guard against existing cyber threats and warnings regarding newly discovered threats.

8. User Responsibility in Host Protection

It is the primary responsibility of the user to regularly update their security software and conduct host security scans. This includes files saved in removable storage devices (e.g., flash drives and mobile hard disk drives).

Apart from the existing gateway security provided by the corporate firewall that scans files downloaded from the Internet and files attached to emails, the user should ensure that it comes from a trusted source.

D. Network

1. Local Area Network

a) Wired Network Connections

A structured local area network has been established for all users to provide optimal network connectivity. IMB personnel/FO RICTMU staff are the only entities authorized to install, remove, or modify network connections and settings. Unauthorized actions will be considered as a breach of security.

b) Wireless Network Connections

Secure Wireless Network Services are available in designated areas within DSWD premises to provide wireless network access to users. A password is required for access and may be requested via email to ICTMS/RICTMU. Password will be changed regularly to maintain security. Existing users will be appropriately advised via email from ICTMS/RICTMU. It is the responsibility of the user not to disclose the password to other users to prevent security issues arising from unauthorized access.

2. Internet

All DSWD users may access the internet within the DSWD building subject to the approved internet use filtering system.

a) *Internet Browser Settings*

The default homepage of all Internet browsers shall be the DSWD website (http://www.dswd.gov.ph) Users must ensure that his/her Internet Browser is updated with the latest available version to increase browsing security coverage. Considering the limitation of internet bandwidth, users are requested to limit tabbed browsing to not more than 5 simultaneous sessions.

b) *Internet Use Monitoring and Filtering*

The IMB shall monitor internet use from all computers and devices connected to the enterprise network. For all traffic, the monitoring system must record the source IP address, the date, the time, the protocol, and the destination site or server. Internet Use records must be preserved for one hundred eighty days (180) days.

c) *Access to Web Site Monitoring Reports*

General trending and activity reports may be made available to support an investigation involving security incidents. This report is considered confidential and must be protected from unauthorized disclosure.

Only the IMB Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary, to respond to a cyber-security incident.

The IMB CSIRT shall be composed of the following:

(1) Chief, Infrastructure Operations Security and Support, IMB- Incident Commander;

(2) Security Administrator;

(3) Network Administrator;

(4) Systems Administrator;

(5) Database Administrator; and,

(6) Web Administrator.

The CSIRT shall report directly to the IMB Director for appropriate disposition.

Internet use reports that identify specific users, sites, or devices will only be made available to entities outside the CSIRT upon written or email request of the Head of OBSU to the IMB Director. This report is considered confidential and must be protected from unauthorized disclosure.

d) ***Internet Use Monitoring and Filtering System***

The IMB shall block access to internet websites and protocols that are deemed inappropriate for DSWD's enterprise environment. Blocked protocols and categories of websites are the following:

(1) Adult/Sexually Explicit Material;

(2) Child Pornography;

(3) Advertisements and Pop-Ups;

(4) Gambling;

(5) Hacking;

(6) Illegal Drugs;

(7) Peer to Peer File Sharing;

(8) Personals and Dating;

(9) Spam, Phishing and Fraud;

(10) Spyware;

(11) Tasteless and Offensive Content;

(12) Violence, Intolerance and Hate;

(13) Gaming Sites; and,

(14) Public Proxy Sites.

e) ***Internet Use Filtering Rule Changes***

The IMB, through the Infrastructure Operations Security and Support Division (OSSD), shall periodically review and recommend changes to web and protocol filtering rules. The IMB Director shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering System Policy.

f) ***Internet Use Filtering Exceptions***

If a site is miscategorized, employees may request the site be unblocked by submitting an email to IMB (netsec@dswd.gov.ph). The IMB will review the request and unblock the site if it is indeed miscategorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit an email request to their Director or Head of Office. The Director or Head of Office will present all approved exception requests to IMB via email. The IMB will unblock that site or category for that associate only. The Infrastructure Operations Security and Support Division of the IMB will track approved exceptions and report on them upon request.

The Chief of IMB's OSSD will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any employee found to have violated this policy may be subjected to disciplinary action.

3. E-mail

All DSWD users shall be provided with an official email account that may be accessed via the web browser or a desktop email client via Post Office Protocol (POP) or Internet Message Access Protocol (IMAP). Users shall be responsible for its maintenance and security.

a) *Usage*

The employee may not use e-mail for purposes that are illegal, inappropriate or disallowed by the DSWD, such as the following*:*

(1) Chain Mail- personal email that attempts to induce the recipient to make a number of copies of the letter and then pass them on to as many recipients as possible;

(2) Harassing or hate mail- any threatening or abusive email sent to individuals or organizations which violates DSWD policies or rules;

(3) Sending 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; and,

(6) Using false identification- any actions that defraud another or misrepresent or fail to accurately identify the sender;

It is the responsibility of the user to maintain his/her emails, i.e. to delete unwanted files, and to save those that are required for archiving.

b) ***Termination of Access Privilege and Waiver***

It is understood that email privileges of the user are terminated upon separation, termination, or other circumstances deemed legal by the DSWD. The IMB requires a notification from the Head of OBSU for appropriate disposition.

VIII. PROHIBITED USAGE AND DISCIPLINARY ACTIONS

A. Prohibited Use

The following uses and acts, discussed thoroughly in Annex D and criminal acts identified in Republic Act 10175 are considered violations in the use of the DSWD ICT facilities and network:

1. Uses contrary to laws, customs, mores and ethical behavior;

2. Uses for personal benefit, commercial, or partisan activities;

3. Acts permitting other users for the unauthorized and/or to benefit personally from the use of the Department's ICT system;

4. Acts that damage the integrity, reliability, confidentiality and efficiency of the ICT system;

5. Acts that encroach on the rights of other users;

6. Acts which violate privacy; and,

7. Specific violations consistent with .existing DSWD policy on progressive disciplining.

IX. ENFORCEMENT PROCEDURES

The IMB in the Central Office and the RICTMU in the Field Offices are designated to monitor compliance of this policy and report violations to the Head, OBSU. They will immediately inform the Director of IMB/Regional Director where the violation occurred using a predefined incident management reporting format (Annex F). 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.

Any DSWD personnel may report any IMB or RICTMU personnel who violates any provision hereof and shall l shall be subject to disciplinary actions after due process.

In cases where there is evidence of serious misconduct or possible criminal activity, appropriate charges shall be filed by the Head of OBSU, through the Legal Service to the proper authorities. This, however, does not prohibit any aggrieved party or complainant other than the Head of OBSU 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 or as a result of investigations, subpoena or lawsuits, DSWD may be required by law to provide electronic or other forms of information and/or records relating to the use of information resources.

X. EFFECTIVITY

This Administrative Order shall take effect immediately and repeals MC 26 series of 2004.

CORAZON JULIANO-SOLIMAN
Secretary

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

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 (!,@,#,$,%/',&,*,(,)_, =+r1/\ ,,'"'<>)

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)

DSWD - the Department of Social Welfare and Development or any of its offices or institutions

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

Hacking Sites - sites that provide content about breaking or subverting computer security controls.

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; the physical component that consists of input devices, central processor, output devices and storage devices

Host Administrator / Root Account - the username or account that has access to all commands and files on a system; has the ability to carry out all facets of system administration (e.g., adding accounts, changing user passwords, installing software and examining log files)

Information and Communications Technology System (ICT System) - includes computers, printers, networks, switches, routers, wireless access points, 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 ICT System may also be considered part of the ICT System

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

Internet Filtering - using technology that monitors each instance of communication between devices on the enterprise network and the Internet and blocks traffic that matches specific rules

IP Address - unique network address assigned to each device to allow it to communicate with other devices on the network or Internet

Multimedia - the use of computers to present text, graphics, video, animation and sound

Network - a group of two or more computer systems linked together. There are many types of computer networks, including: Local Area Network (LAN), which is a computer network limited to the immediate area, usually the same building or floor of a building, and Wide Area Network (WAN), which is meant to cover a wide geographic area, pertains to the physical network to all DSWD offices nationwide

Operating System - a 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

Peer-to-Peer File Sharing – services or protocols such as Torrent, which allow internet-connected hosts to make files available to or download files from other hosts

Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication

Server - a computer with a running instance of an application capable of accepting requests from the client and giving responses accordingly

Simple Mail Transfer Protocol (SMTP) - the Internet Protocol that facilitates the exchange of mail messages between internet mail servers

Social Networking Services - internet sites such as Facebook and Twitter that allow users to post content, chat, and interact in online communities

Software - a set of instructions to a computer to execute a command to 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

Tasteless and Offensive Content - Content that is gratuitously offensive or shocking, but not violent or frightening. Includes sites devoted in part or whole to scatology and similar topics or to improper language, humor or behavior

Spam - are website links from unsolicited Internet mail messages

User ID - an identifier or a handle for a user on the Internet or Network; also known as username

Users - refers to one or more of the following: (1) current employees of DSWD—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 ICT resource by DSWD.

Virus - a computer program that can copy itself, infect and disrupt a computer software

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

Annex B: CURRENT HARDWARE STANDARDS

Effectivity: 4th Qtr 2014

A. Computers:

Component	Computer Form Factor		
	All-In-One Desktop[1]	**Workstation[2]**	**Ultrabook[3]**
Processor	Multi Core w/ at least 3MB Cache Latest Processor Architecture for Business Must have embedded security feature on the CPU to be able to remotely manage, monitor and report status of each PC	Multi Core w/ at least 6MB Cache Latest Processor Architecture for Business Must have embedded security feature on the CPU to be able to remotely manage, monitor and report status of each PC	Multi Core w/ at least 6MB Cache Latest Processor Architecture for Business Must have embedded security feature on the CPU to be able to remotely manage, monitor and report status of each PC
Operating System	Latest Proprietary OS for Corporate Application 64-Bit Enterprise Edition	Latest Proprietary OS for Corporate Application 64-Bit Enterprise Edition	Latest Proprietary OS for Corporate Application 64-Bit Enterprise Edition
Office Productivity Software	Latest Proprietary Office Productivity Tools for Corporate Application Pro Edition (Word Processor, Spread Sheet, Presentation, Email Client, Database Engine)	Latest Proprietary Office Productivity Tools for Corporate Application Pro Edition (Word Processor, Spread Sheet, Presentation, Email Client, Database Engine)	Latest Proprietary Office Productivity Tools for Corporate Application Pro Edition (Word Processor, Spread Sheet, Presentation, Email Client, Database Engine)
Memory	≥4096 Mb	≥4096 Mb	≥8192 Mb
Keyboard	Wireless Keyboard (same brand as PC)	Standard English (same brand as PC)	Built-in w/ backlight
Pointing Devices/Mouse	Wireless with 2 button + scroll Mouse (same brand as PC)	Standard Optical USB with 2 button + scroll Mouse (same brand as PC)	Touch Pad + Wireless with 2 button + scroll Mouse (same brand as PC)
Video Graphics Controller	≥ 512 Mb Integrated DVI + HDMI	≥ 512Mb Discrete DVI + HDMI	Integrated with Micro HDMI + mini VGA with adaptors
Monitor	≥23" LED IPS Multi Touch Technology	≥18" LED	≥11", ≤ 14" LED, Multi Touchscreen Technology
Hard Drive	≥500Gb, 7200 rpm Serial ATA	≥ 1 Tb, 7200 rpm Serial ATA	≥128Gb SSD
Sound Card	Integrated	Integrated	Integrated
Network Controller	Integrated 10/100/1000 Base-T Ethernet+ WLAN 802.11. b/g/n, Bluetooth 4.0	Integrated 10/100/1000 Base-T Ethernet+ WLAN 802.11. b/g/n	WLAN 802.11 b/g/n + Integrated 10/100/1000 Ethernet or 10/100/1000 Ethernet adaptor

1 All-in-One Desktop - personal computer for office productivity can be mobile
2 Workstation - enhanced desktop designed for highly technical and multimedia applications
3 Ultrabook – small, mobile computer, weighing 1-4 kilograms.

Component	Computer Form Factor		
	All-In-One Desktop[1]	**Workstation[2]**	**Ultrabook[3]**
I/O Ports	≥ 2 USB 3.0 ports, ≥ 2 USB 2.0 ports	≥ 2 USB 3.0 ports, some on the front of the computer	≥ 1 USB 3.0 ports
Expansion slots	7 in 1 Memory Card Reader	≥2 PCI/PCIE	N/A
Optical drives	DVD-RW	DVD-RW	N/A
CPU Power Supply	Built-in, should be appropriate with all-in-one desktop, with AC adaptor	Built-in, should be appropriate for the Workstation	Built-in, should be appropriate for the Ultrabook
UPS (Battery for Notebook)	≥ 500 VA with AVR; Warranty and Replacement for the battery 1 Year, UPS socket should be compatible with the all-in-one AC Adaptor	≥ 500 VA with AVR; Warranty and Replacement for the battery 1 Year, UPS socket should be compatible with the Workstation	(≥ 6 cell Lithium Ion)
Security Software	NA (Corporate AV)	NA (Corporate AV)	NA (Corporate AV)
Warranty & SLA	3 years Hardware Warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service center per region; On-call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time	3 years Hardware Warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service center per region; On-call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time	1 year Hardware Warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service center per region; On-call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time
Other Requirements	Manufacturer must be ISO 9000 (or higher) certified; Manufacturer must be 14000 (or higher) certified; Must be energy star compliant; Manufacturer must have a website that provides service helpdesk and includes downloadable software drivers and utilities; Manufacturer must be included in the latest report of the following:	Manufacturer must be ISO 9000 (or higher) certified; Manufacturer must be 14000 (or higher) certified; Must be energy star compliant; Manufacturer must have a website that provides service helpdesk and includes downloadable software drivers and utilities; Manufacturer must be included in the latest report of the following:	Manufacturer must be ISO 9000 (or higher) certified; Manufacturer must be 14000 (or higher) certified; Must be energy star compliant; Manufacturer must have a website that provides service helpdesk and includes downloadable software drivers and utilities; Manufacturer must be included in the latest report of the following:

Component	Computer Form Factor		
	All-In-One Desktop[1]	**Workstation**[2]	**Ultrabook**[3]
	- Leader or Challenger Quadrant of Gartner's Magic Quadrant - Top five (5) of International Data Corporation (IDC) report; Manufacturer must be included in the latest available top five (5) list of Gartner's Worldwide PC vendor Unit shipments; Manufacturer must be included in the latest IDCs top five (5) vendors in terms of worldwide PC shipments; The service provider must be engaged in the industry of ICT Hardware, Software and Solutions	- Leader or Challenger Quadrant of Gartner's Magic Quadrant - Top five (5) of International Data Corporation (IDC) report; Manufacturer must be included in the latest available top five (5) list of Gartner's Worldwide PC vendor Unit shipments; Manufacturer must be included in the latest IDCs top five (5) vendors in terms of worldwide PC shipments; The service provider must be engaged in the industry of ICT Hardware, Software and Solutions	- Leader or Challenger Quadrant of Gartner's Magic Quadrant - Top five (5) of International Data Corporation (IDC) report; Manufacturer must be included in the latest available top five (5) list of Gartner's Worldwide PC vendor Unit shipments; Manufacturer must be included in the latest IDCs top five (5) vendors in terms of worldwide PC shipments; The service provider must be engaged in the industry of ICT Hardware, Software and Solutions

B. Tablets:

	Tablet	2 in 1 Ultrabook Computer
Processor	≥ 1.3Ghz Multi Core Latest Processor Architecture for Business	Multi Core w/ at least 4MB Cache Latest Processor Architecture for Business
Operating System	Latest Open Source Operating System	Latest Proprietary OS for Corporate Application 64-Bit Enterprise Edition
Office Productivity Software	Mobile Encoding Application	Latest Proprietary Office Productivity Tools for Corporate Application Pro Edition (Word Processor, Spread Sheet, Presentation, Email Client, Database Engine)
Memory (RAM)	≥2048 Mb	≥4096 Mb
Keyboard	Built-in through touch screen	Detachable, Flip able and twistable + Wireless keyboard cover with clickable touchpad
Pointing Devices/Mouse	Capacitive Touch screen	Touch Pad + Wireless with 2 button + scroll Mouse
Video Graphics Controller	Integrated	Integrated with Micro HDMI inclusive of adaptors
Screen/Monitor	At least 7" IPS Multi touch technology	≥11", ≤ 14" LED, Multi Touchscreen Technology
Camera	Front Facing: Optional Rear Facing: At least 3.0 Megapixels	At least 3.0 Megapixels
Internal Storage / Hard Drive	≥16Gb in total (RAW) ≥12Gb useable	≥128Gb SSD
Sound Controller/Card	Integrated	Integrated
Network Controller	WLAN 802.11 b/g/n + Bluetooth 4.0 Wireless Technology + 3G	WLAN 802.11 b/g/n + Integrated 10/100/1000 Ethernet or 10/100/1000 Ethernet adaptor
I/O Ports	At least Standard SIM Card tray with Micro, Mini and Nano SIM Adaptors	≥ 1 USB 3.0 ports
Weight	≤ 1kg	≤ 1.8 kg
Security Software	NA (Corporate AV)	NA (Corporate AV)
Warranty & SLA	1 year Hardware Warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service center per region; On-call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time	1 year Hardware Warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service center per region; On-call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time
Other Requirements	Manufacturer must be ISO 9000 (or higher) certified; Manufacturer must be 14000 (or higher) certified; Must be NTC approved; The service provider must be engaged in the industry of ICT Hardware, Software and Solutions	Manufacturer must be ISO 9000 (or higher) certified; Manufacturer must be 14000 (or higher) certified; Must be energy star compliant; Manufacturer must have a website that provides service helpdesk and includes downloadable software drivers and utilities; Manufacturer must be included in the latest report of the following:

		- Leader or Challenger Quadrant of Gartner's Magic Quadrant - Top five (5) of International Data Corporation (IDC) report; Manufacturer must be included in the latest available top five (5) list of Gartner's Worldwide PC vendor Unit shipments; Manufacturer must be included in the latest IDCs top five (5) vendors in terms of worldwide PC shipments; The service provider must be engaged in the industry of ICT Hardware, Software and Solutions

C. Printers:

	All in One Printer	Laser Printer	Digital Multi-Function System
OS Compatibilty	Windows, Linux, Unix, Macintosh	Windows, Linux, Unix, Macintosh	Windows, Linux, Unix, Macintosh
Warm up Time	N/A	N/A	≤ 1 minute
Memory (RAM)	≥ 32Mb	≥ 32Mb	≥ 1Gb
Monthly Duty Cycle	≥ 5000 impressions	≥ 30,000 impressions	≥ 200,000 pages
Copy Speed	≥ 18 cpm (black); ≥ 15 cpm (colored)	N/A	≥ 45 cpm (black); 30 cpm (colored)
Copy Resolution	600 dpi (black) 1200 (colored)	N/A	600 dpi (black); 600 dpi (colored)
Continuous Copy	999	N/A	999
Copy Magnification Zoom	25 to 400% (in incremental of 1%)	N/A	25 to 400% (in incremental of 1%)
Print Technology	N/A	Laser	Laser
Print Speed	≥ 18 ppm (black); ≥ 15 ppm (colored)	≥ 20 ppm (black); ≥ 20 ppm (colored)	≥ 45 ppm (black); 30 ppm (colored)
Print Resolution	4800 x 1200 dpi	600 x 600 dpi	600 x 600 dpi
Duplex Copying/Printing	Yes	Yes (Printing Only)	Yes
Scanning Optical Resolution	1200 dpi	N/A	600 x 600 dpi
Scanning Bit Depth	≥ 24 bit	N/A	N/A
Max Scan Size (ADF)	Legal	N/A	A3
Supported File Format in Scanning	PDF, TIFF, JPEG	N/A	PDF, TIFF, JPEG
Scan Destination	To Email, Computing Device, FTP, USB port	N/A	To Email, Computing Device, FTP, USB port
Fax Transmission Speed	At least 33.6 kbps	N/A	At least 33.6 kbps
Fax Resolution	300 x 300 dpi	N/A	300 x 300 dpi
Fax Compression Method	MH, MR, MMR, JBIG	N/A	MH, MR, MMR, JBIG
Fax Communication Protocol	Super G3 / G3	N/A	Super G3 / G3
Document Feeder Sheet Capacity	At least 20 sheets	N/A	At least 100 sheets
Document Feeder Max Size Capacity	Legal	Legal	A3
Max Copy Size	Legal	N/A	A3
Paper Tray Sheet Capacity	At least 100 sheets	At least 100 sheets	At least 2 x 500 sheet tray
Connectivity	Hi-Speed USB 2.0; Ethernet 10/100/1000 Base-T; WLAN 802.11 b/g/n	Hi-Speed USB 2.0; Ethernet 10/100/1000 Base-T; WLAN 802.11 b/g/n	Hi-Speed USB 2.0; Ethernet 10/100/1000 Base-T; WLAN 802.11 b/g/n; Standard PCL 6/5e
Warranty & SLA	1 year Hardware Warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service center per region; On-	1 year Hardware Warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service center per region; On-	1 year Hardware Warranty; Lifetime service warranty; Must be capable of support Nationwide deployment and with at least 1 or more accredited by the manufacturer service

	call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time	call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time	center per region; On-call and on-site support must be available 24/7 including holidays; Response time is within 2 hours. Resolution time must be within (1) calendar day for NCR and two (2) calendar days for other regions; A service unit must be provided if parts are not available and the resolution time exceeds the specified time

Annex C: LIST OF AUTHORIZED SOFTWARE

Effectivity: 4th Qtr 2014

Class	Proprietary Software	FOSS
Client Operating System	Microsoft Windows Macintosh OSX	PCLinux Ubuntu
Server Operating System	Microsoft Windows Server	CEntOS RHELinux Ubuntu
Business Productivity Tools	Microsoft Office Microsoft Word Microsoft Excel Microsoft Powerpoint Microsoft Visio Microsoft Project	Open Office Writer Calc Impress
Document Imaging	Microsoft Office Document Imaging	
Anti-Virus	Kaspersky Anti-Virus	
PDF converter	Acrobat	PrimoPDF free
PDF reader	Acrobat Reader	Foxit PDF
Electronic Mail Client	Microsoft Outlook /OExpress	Mozilla Thunderbird
Firewall	Kaspersky Firewall	
Database Server Software	MS SQL Server Oracle xG Microsoft Access	MySQL PostgreSQL
Web Server Software	IIS	Apache
Internet Browser	Internet Explorer	Mozilla Firefox Google Chrome Opera Safari
Development Platform	MS Visual Studio	PHP JBoss Java
Statistical Package	SPSS	
Encryption	Microsoft Bit-Locker	
Utilities	WinZip, WinRAR	7zip
Multimedia	Adobe Suite Macromedia Suite Microsoft	

Annex D: PROHIBITED ACTS AND USES OF THE ICT RESOURCES

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

Criminal Use

- Use of DSWD ICT resources for criminal activities
- Use of copyrighted material

  Prohibited acts include but are not limited to:
  - 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 ICT System);
  - Infringement of intellectual property rights belonging to others through the use of telecommunications networks (This is a criminal offense under Section 33(b) of the Electronic Commerce Act);
  - Cheating;
  - 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; and,
  - 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.

Uses for Personal Benefit, Business or Partisan Activities

Commercial Use

- Use of the ICT System for commercial purposes, and product advertisement, for personal profit, unless permitted under with the written approval of a competent authority

Use of the ICT resources for any religious and 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 DSWD

Games and Entertainment

- Use of ICT resources to play games, or any activity unrelated or inappropriate to the duties and responsibilities of the user

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

- Unauthorized deletion, removal, modification, installation and/or destruction of any computer equipment, peripheral, operating system, disk partition, software, database, or other component of the ICT System
- Connection of any computer unit or external network to the ICT System without the permission of the ICTMS
- Attempt to crash, tie up, or deny any service on the ICT System, through acts 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, and, sending data packets that serve to flood the network bandwidth
- 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
- Concealment of identity or masquerading as other users when accessing, sending, receiving, processing or storing through or on the ICT System

Acts that Encroach on the Rights of Other Users

- Sending unsolicited mail such as chain letters, advertisements, jokes, trivia, announcements to non-official groups or activities, offers, inquiries, and the like (i.e., spamming)
- Accessing, downloading, producing, disseminating, or displaying material that could be considered offensive, obscene, pornographic, racially abusive, culturally insensitive, or libelous in nature
- Sending messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of DSWD
- Interfering with or disrupting other computer users through acts such as, but not limited to, sending messages through pop-up screens, running programs that simulate crashes, and running spyware to monitor activities of other users

Acts which violate privacy

- Hacking, Spying or Snooping
    - 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.)
    - Decrypting, attempting to decrypt, or enabling others to decrypt such information which are intentionally encrypted, password- protected, or secured (Encrypted data are considered confidential, and include, but not limited to: passwords, digital keys and signatures.)

    - Re-routing or capture of data transmitted over the ICT System
    - 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
- Unauthorized Disclosure
    - Copying, modification, dissemination, or use of confidential information such as, but not limited to, mailing lists and personal identifiable information of any sort without permission of the person or body entitled to give it
    - 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
- 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:
    - Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;
    - 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.;
    - Any material that permits an unauthorized use-, who has gained access to a system, to carry out any modification of the computer programs or data stored in the system; and,
    - Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system.

ANNEX F: INCIDENT MANAGEMENT REPORT FORMAT

Date

ICT Incident Management Report

For: Head of Office

From: IMB/RICTMU

Incident/Issue /Problem-

Observed Date and Time:

Location:

Services affected:

IMB/RICTMU interventions

Recommendation-

IMB/RICTMU