0917. 13DPWH
01.29.2015

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
OFFICE OF THE SECRETARY
MANILA

JAN 28 2015

DEPARTMENT ORDER)
)
NO. 13)
Series of 2015 01.29.15

SUBJECT: Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources

The Department provides its officials and employees with ICT resources and services for the effective performance and fulfillment of their respective tasks and responsibilities. These resources are intended to support the Department's legitimate business requirements.

In order to ensure the proper use of the DPWH ICT resources, the attached **Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources** is hereby mandated for the guidance and compliance of all concerned.

This Order supersedes Department Order No. 20, Series of 2007 and shall take effect immediately.

ROGELIO L. SINGSON
Secretary

4.5.2 RGG/NSP

Department of Public Works and Highways
Information Management Service

Policies and Guidelines

on the use of

DPWH
Information and Communication Technology (ICT)
Resources

Revision No. 1.0
January 14, 2015

Table of Contents

Acronyms

BYOD	Bring your own device
DPWH	Department of Public Works and Highways
ICT	Information and Communication Technology
IT	Information Technology
ID	Identification
IMS	Information Management Service
OWA	Outlook Web App
POD	Personally-owned device

1. Purpose

The appropriate and legitimate use of Information and Communication Technology (ICT) resources is a vital concern for an organization. The purpose of this document is to define the policies and guidelines for users who have valid business requirements to use or access the DPWH ICT resources.

The provisions contained herein are intended to protect the security and integrity of the DPWH ICT resources, and to guide and establish the responsibilities of users on the proper use of these resources.

2. Scope

This Policies and Guidelines on the use of DPWH ICT Resources applies to all users (employees, suppliers, consultants, guests, etc.) of ICT resources owned and managed by the DPWH.

3. Definition of Terms

3.1. Application System

A system to which a computer program or software is applied, such as Civil Works Registry (CWR) and Document Tracking System (DoTS).

3.2. Bring your own device (BYOD)

A scheme that allows users to bring and use their own computing devices to accomplish work for the DPWH.

3.3. Data File

A collection of data accumulated for a definite use, such as Word Processing Documents, Spread Sheets, Databases, etc.

3.4. ICT Resources

The DPWH ICT resources include all hardware and software owned, licensed or by agreement, leased or managed by DPWH, data/files, telephone, intranet, internet, email and application system.

3.5. Hardware

All equipment involved in the operations of a computer system which includes, but not limited to, computers, mobile devices, data communications equipment, workstations, and various peripherals such as printers and plotters.

3.6. Head of Offices

Officials with the rank of Division Chiefs, Assistant District Engineers, District Engineers, Assistant Regional Directors, Regional Directors, Project Directors, Assistant Bureau Directors, Bureau/Service Directors, and higher.

3.7. Information and Communication Technology (ICT)

Often used as an extended synonym for Information Technology (IT), but is a more specific term that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.

3.8. Internet

A large computer network linking smaller computer networks worldwide.

3.9. Intranet

A computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization.

3.10. Login ID

A string of characters that uniquely identifies a user and allows access to a computer system, communication network and application systems.

3.11. Mobile devices

Computing devices that include, but not limited to, laptop computers, tablet computers, and smartphones.

3.12. Network Domain

An interconnected set of computer hardware peripherals and devices.

3.13. Personally owned device (POD)

A device owned by a user and third parties to produce, modify or view DPWH data.

3.14. Software

All programs involved in the operation of a computer system which include, but not limited to, operating systems, data communications software, database management systems and applications software.

3.15. User

All DPWH employees and third parties such as consultants, suppliers, maintenance contractors, and others who were granted access to, and use of, the DPWH ICT resources.

3.16. Workstation

A computer designed for technical or scientific applications intended primarily to be used by one person at a time, and is commonly connected to a local area network and run multi-user operating systems.

4. Duties and Responsibilities

The following are the duties and responsibilities of everyone concerned in the implementation of the Policies and Guidelines for the Use of DPWH ICT Resources:

4.1. All Users

All users shall adhere to the policies and guidelines prescribed herein. Failure to do so may lead to loss of privileges and/or disciplinary action as provided under Section 5.8 of this Policy Guideline. Users are also responsible for reporting ICT-related problems to the IT Service Desk.

Users should exercise care to safeguard the equipment assigned to them. Users are accountable for any loss or damage that may result due to negligence.

Users are responsible for the back-up of their own files on workstations.

Users who work on non-DPWH-owned computers and are outside the control of IMS should not use Department-owned/licensed software and must adhere to the policy on data security provided under Section 5.6 of this Policy Guideline.

Users should ensure that these computers are free from viruses before copying files back to the Department's computers.

Users should practice regular scanning of their files and external storage devices and to frequently check if their anti-virus definition file is up to date. In the event of virus infection or outdated (beyond 7 days from the current date) anti-virus definition files, users should report immediately to the IT Service Desk.

4.2. Division and Section Chiefs

All supervisors are responsible for ensuring that their subordinates follow the provisions of this Policy Guideline.

It is their responsibility to monitor and control the activities of their staff pertaining to the use of DPWH ICT resources and ensure that they are employed for their intended purposes. They shall report to the IMS any violation of this Policy Guideline.

Supervisors should ensure that new employees are given orientation on these Policies and Guidelines and are made aware of their corresponding duties and responsibilities in using these ICT resources.

4.3. Information Management Service (IMS) and Regional/District IT Support Officers

IMS shall set the rules and regulations for the installation of duly authorized and approved hardware, software and other peripherals owned by the DPWH, including the maintenance and security of data and network equipment; and, formulation and implementation of a disaster recovery plan relating to IT.

IMS and the Regional/District Support Officers shall remove all unauthorized hardware and/or software connected to/installed in the DPWH ICT Infrastructure and recommend sanctions to employees violating the guidelines under Section 5.8 of this Policy Guideline.

IMS and the Regional/District IT Support Officers shall back up data on the server and ensure that it is readily available for restoration in the event of a disaster or interruption occurring during normal operation.

IMS and the Regional/District IT Support Officers shall only maintain telephones/fax machines connected to the communication network and will not be liable for those provided by external telephone companies and are not owned by the Department.

IMS and the Regional/District IT Support Officers shall only maintain and provide security for the Department's centralized internet connection and email system and will not be liable for any security breach/threats incurred from using portable or wired broadband internet connections and 3rd party email systems.

4.4. IT Service Desk

The IT Service Desk is the single point of contact between users and the technical support team of IMS. They are responsible for handling incident reports, service request management, and providing solutions to IT-related problems/issues. Users may contact the IT Service Desk thru its hotline number 43070 (external number 304-3070), thru email at itservicedesk@dpwh.gov.ph, or thru the DPWH IT Service Desk Customer Portal (http://itservicedesk/footprints).

5. General Policy

5.1. Monitoring and Privacy

The DPWH reserves the right to monitor and review the web access, files, emails, and other information stored on the user's computers, as necessary, in order to ensure the integrity of these systems and users' compliance with all relevant policies and guidelines.

The DPWH reserves the right to inspect and examine any and all IT equipment (including personally owned equipment) used for the conduct of official business within or outside official premises, or connected in any way to the DPWH network, to ensure compliance with the DPWH Policies. Users who bring into the workplace personal IT equipment, including laptop computers, or any other mobile device, any such equipment or device, and data held thereon, agree that these may be inspected at any time by IMS representatives to ensure that these do not pose risk/s to DPWH whether by way of virus infection, hacking, intrusion or the presence of improper, offensive or illegal materials.

Users of DPWH ICT resources should be aware and accept, as condition of use that such facilities whether used for official business or personal purposes will be monitored.

5.2. Establishing and Maintaining Corporate Identity and Image

The Department prescribes the use of its official email (**@dpwh.gov.ph**) in communicating and transacting official business with other entities in order to establish and maintain its corporate identity.

Since users carry the name of DPWH each time they use official ICT channels of communication, prudence must be diligently observed. Users expressing personal opinions or taking a personal stand on issues, when using official ICT channels must explicitly state that what he/she expressed is not representing DPWH.

5.3. Permitted Use of ICT Resources

The DPWH ICT resources is intended to support the Department's legitimate business requirements. Occasional and reasonable use of the DPWH ICT resources for personal purposes is regarded as acceptable provided that:

- These are not used for illegal activities or for private business or other commercial purposes including the sale or purchase of goods and services;
- It is not done during working hours; and
- It does not interfere with the performance and accomplishment of the user's duties and responsibilities.

5.4. Restrictions on the Use of ICT Resources

DPWH forbids the use of its ICT resources for any purpose that could blemish its institutional image and/or strain its operational efficiency or compromise its security and integrity. For this reason, the following are strictly prohibited:

- sharing/saving offensive content of any kind, including pornographic material;
- promoting discrimination on the basis of race, sex, age, sexual orientation, religion, disability, social status, etc.;
- harassment, threats or violent behaviour;
- gambling, theft, piracy and other illegal/fraudulent activities;
- personal financial gain;
- activities that reduce the productivity of users, e.g. playing games, watching movies, video streaming, etc.;
- system hacking or deliberately propagating computer viruses, worms, Trojan, etc.;
- accessing and/or dispensing confidential data/information without authorization; and,
- any activity that violates any government law, code or policy.

5.5. Request and Approval Procedure

5.5.1. Request for Access

Access to the DPWH ICT resources shall be granted to users upon the formal request of their Head of Office and approval of IMS. Access request forms included in Section 14 of this Policy Guideline can be downloaded from the DPWH intranet website - download page (http://dpwhweb/downloads/index.htm).

Users must sign the statements located on the last page of each access request form to signify that he/she understands and agrees to comply with all relevant DPWH ICT policies.

Requests shall be approved only if reasonable business needs are identified and shall be granted based on the employee's job responsibilities which involves, but not limited to the following:

- research, education and training;
- calamity and disaster operations;
- updating of technical documents and gathering of best practices from different external entities;
- regular downloading/uploading of data from external offices or agencies;
- regular communication and/or submission of reports with internal and external offices; and,
- user of the Department's application systems.

Officials with the rank of Assistant District Engineers, District Engineers, Assistant Regional Directors, Regional Directors, Project Directors, Bureau Assistant Directors, Bureau/Service Directors and higher shall be automatically given telephone lines, intranet, internet and email access upon signing of the agreement stated on the request form.

5.5.2. Approval

The access request form should be signed by the user's Head of Office and submitted to the IT Service Desk for processing. IMS shall review the submitted access request form and take appropriate action.

5.6. Data Security and Accountability

Data should always be secured in terms of:

- Confidentiality – protection of information from unauthorized disclosure to external entities or from those who are not entitled to access the information, through improper or careless disposal techniques;
- Integrity – protection of information from unauthorized modification or manipulation, and ensure that information is accurate and complete.

5.7. Revocation of Privileges

Access to DPWH ICT resources shall be discontinued upon termination of employment (resignation, retirement, dismissal, completion of contract, etc.), or during disciplinary action arising from violation of this Policy.

In case of change in job function and/or transfer, the original access privilege shall be discontinued and an approved request form shall be submitted to the IT Service Desk for the new access privileges.

E-mail accounts that have been inactive for forty-five (45) days shall be automatically revoked. The user is required to submit an approved request form to the IT Service Desk to reactivate the account.

DPWH reserves the right to revoke user's ICT privileges for any violation of this Policy Guideline at any time and without prior notice, and impose sanctions stipulated in Section 5.8.

5.8. Sanctions

Pursuant to the expressed provisions of Section 22 (c), Rule XIV, Book V of Executive Order No. 292, series of 1987, the corresponding penalties for violation of reasonable office rules and regulations shall apply:

1st offense	-	Written reprimand
2nd offense	-	Suspension for one (1) to thirty (30) days
3rd offense	-	Dismissal

6. Hardware

6.1. Scope

Covers all Department-owned or leased IT equipment including installed physical components, accessories, parts or peripherals.

6.2. Policy

The IMS may authorize the use of specialized hardware other than those provided in the standard equipment. No computer or network hardware may be installed without the approval of the IMS. This includes, but not limited to, internal cards, routers, Wi-Fi, switch, USB broadband or other devices that can be connected to workstations and servers.

Only authorized IMS representatives shall perform all types of equipment installations, disconnections, modifications, and relocations of ports and cables.

All computers, laptops, servers and network printers should be configured and connected to the Department's network domain.

All ICT equipment (except for those that are located in the network room and floor distributors) should be properly turned-off after office hours when not in use to save on electricity and to extend the life of the equipment.

Shared portable equipment such as laptops or workstations shall not be taken out of the Department without the informed consent of the concerned supervisor. Informed consent means that the supervisors know what equipment is being taken out, what data is on it, and for what purpose it will be used.

7. Software

7.1. Scope

Covers all Department-owned or subscribed applications or software whether commercial, in-house developed or open source.

7.2. Policy

Installation or use of unauthorized/unlicensed, non-standard software, including personally owned software, is prohibited. Only software that is licensed to or owned by the Department is to be installed on the Department's computers. It is the Department's policy to abide with all the laws and regulations regarding copyright and Intellectual Property Rights (IPR) Law.

All software (package, programs or applications), data, and data files loaded on the Department's computer systems are the properties of the Department. As such, the Department retains the right to access, copy, and change, alter, modify, destroy, delete or erase any of these properties including free-to-use software installed by IMS.

Software or applications licensed to the Department shall not be installed on personal devices. Users are also prohibited to use the Department's software licenses on their personal device/s or to distribute it to individuals not officially connected to the DPWH.

Downloading and installation of any software, either freeware or shareware, shall not be allowed unless authorized by the IMS. A request form must be accomplished and coursed through the IT Service Desk.

8. Telephone System

8.1. Scope

Covers all Department-owned or leased telephone/fax machine equipment connected to the communication network.

8.2. Policy

In addition to the provisions under Section 5.4 of this Policy Guideline, the following activities are also strictly prohibited:

- use of any equipment or service for autodialing, continuous or extensive call forwarding or to connect to any device that permits the services to be used as an outbound trunk by more than one individual;
- use of the service for telemarketing or fax broadcasting;
- tampering of the equipment to gain access to other features;
- bringing the equipment outside the DPWH premises without approved consent from the supervisor;
- violates the privacy of others; and
- does not adhere to proper phone etiquettes.

9. Intranet Access

9.1. Scope

The DPWH intranet or wide area communication network (WAN) is used for both voice and data communications. The WAN originates in the Central Office and utilizes leased lines to connect to the Regional and District Engineering Offices. The intranet enables users to access the DPWH ICT resources which include the telephone system, websites, applications, internet, email, data and other shared resources.

9.2. Policy

In addition to the provisions under Section 5.4 of this Policy Guideline, the following activities are also strictly prohibited:

- unauthorized accessing of DPWH data or files of other employees;
- using the log-in ID of other employees;
- unauthorized broadcasting of bulk messages to all users; and,
- sharing or transferring of large files across the network that are not relevant to the business operations of the Department.

9.3. Login IDs and Password

Upon approval of the access request form, the user shall be given a log-in ID to access the intranet and other DPWH ICT resources. The user is responsible and accountable for all activities carried out under his/her log-in ID. The standard DPWH login ID is a combination of the user's last name, first letter of the first name and the first letter of the middle name.

The password is the user's personal key to access the DPWH ICT resources. The default password given by the IMS must be immediately changed to a personal password to safeguard against unauthorized access to a user's account. Passwords also help ensure that only the authorized person is accountable for all transactions and other changes made to system resources, including data.

9.3.1. Confidentiality

Log-in IDs and/or passwords should never be shared with anyone and should not be written down and left in a place accessible to unauthorized persons. Failure to observe caution exposes the user to the risk of another person using his/her log-in ID and password.

Users are automatically prompted by the system to change password every forty-five (45) days. In the event of an expired password, the user may request for the IMS to reset his/her password thru the IT Service Desk. If access to a log-in ID is required in the absence of the owner, a written consent signed by the user's supervisor or head of office must be presented to the IMS.

9.3.2. Password Construction

Password must meet the following complexity requirements for security:

- should be at least eight characters;
- combination of upper and lower case letters, numbers and special characters;
- should not be the same as user's log-in ID or an anagram of it; and,
- should avoid obvious and easy to guess words such as, "password", "abcd1234", birthdays, names and the like.

9.3.3. Account Lock-out

For security, log-in IDs will be locked-out after five (5) invalid logon attempts. Invalid password attempts on computers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers are counted as failed logon attempts. A locked-out log-in ID cannot be used until it is unlocked by the IMS or until the lockout duration of fifteen (15) minutes has expired.

9.4. Temporary Deactivation of Log-in ID due to Vacation or Extended Leave

A user who will be away from the office for a period of more than two (2) months and does not intend to access his/her log-in ID, may request for its temporary deactivation to ensure that no one will be able to use the user's log-in ID while he/she is away.

10. Internet Access

10.1. Scope

Covers internet services accessed on any workstations and servers under the jurisdiction and/or ownership of the Department whether these computers are connected to the DPWH communications network or stand-alone workstations.

10.2. Policy

Servers and computers configured to the Department's network domain should not be connected to a different internet connection other than the one provided by IMS.

In addition to the provisions under Section 5.4 of this Policy Guideline, the following activities are also strictly prohibited:

- Accessing sites that may compromise the security of the Department's communications network, e.g. external web mails, malicious websites, torrents, porn sites, shareware sites, etc.;
- Accessing sites that reduce the productivity of the users, e.g. gaming sites, social networks, chat, video streaming, etc.. However, access to Facebook and Twitter will be allowed with limited functionalities during office breaks (12:00 noon to 1:00 pm) so as not to disrupt the users work;
- Downloading of files that may introduce virus or malwares, e.g. pirated software, shareware, freeware, etc.; and,
- Activities that may put unnecessary strain on the internet bandwidth, e.g. downloading of large files, file sharing sites, torrents, video streaming, video calls, etc.

11. Email Access

11.1. Scope

Covers Email services located on any workstations and servers under the ownership and/or jurisdiction of the Department whether accessed through or outside the Department's communication network.

11.2. Policy

In addition to the provisions under Section 5.4 of this Policy Guideline, the following activities are also strictly prohibited:

- forward, send or store emails and other files of inappropriate and/or illegal contents;
- forward or send chain letters;
- forward or send emails with large attachments to multiple users;

- use of email for promotion or campaign during elections and other partisan activities;

- forward or send files containing viruses, spams and other malicious files; and,

- use of email for subscribing to any website that are not relevant to one's work or the Department's operations.

11.3. Email Accounts

Upon approval of the Request for Intranet Access, users are automatically given email access that can be used to send and receive email within (internal) the Department. If the user requires to send and receive email outside (external) the Department, the user needs to submit a request as stated in Section 5.5.1 of this Policy Guideline.

11.4. Outlook Web App (OWA)

OWA is the web-based version of the Department's email system which is accessible internally through the Department's communication network and externally via internet connection using web browsers like Microsoft Internet Explorer, Mozilla Firefox or Safari, using the following links:

- within DPWH: https://mail.dpwhnet.gov.ph/owa

- outside DPWH: https://mail.dpwh.gov.ph/owa

Use caution especially when accessing OWA from public internet facilities like internet cafes which are prone to viruses and other security threats. Always keep in mind the following:

- select the option "This is a public or shared computer;"

- When logging in using portable devices, make sure that no one is able to capture your login ID and password; and,

- always logout from OWA and close browser sessions when done.

11.5. Mailbox Quotas

A mailbox is a storage area where emails are saved. User mailbox capacity are assigned as follows:

Type of User	Mailbox Size
Executive Committee Members	1,000 MB
Bureau/Service/Regional Directors	1,000 MB
Others	200 MB

11.6. Maximum Number of email Recipients

Users are restricted to 20 recipients per message to ensure optimal performance of the email system. This may be increased if necessary, subject to the approval process.

11.7. Message and Attachment Size Limits

By default, all users can send and receive email messages with attachment (internal and external) not exceeding 10 MB. Attachment larger than 10 MB (internal up to 50 MB and external up to 20 MB) may be allowed if necessary, subject to the approval process.

11.8. Exchanging Large Files

Users can exchange large files internally without depleting the Department's email system by copying files onto a public folder on a DPWH file server, and informing the intended recipient (preferably by e-mail) of the location and name of the file.

All users are given access to a Temporary File Sharing Area which is mapped as drive Z:\Temp_File_Sharing in Windows Explorer. Users can copy any file that they wish to exchange with others into the appropriate sub-folder in this area.

This is a temporary storage area only and should not be used for backup purposes or as a working area. Files on this server are automatically deleted every Friday at 7:00 pm to free up storage space. It is therefore the responsibility of the user to keep a backup copy of their files in their respective hard drives.

12. Application Systems Access

12.1. Scope

Covers all application systems or software - whether in-house developed, outsourced, provided by consultants, or procured off-the-shelf - that generate or have access to the Department's data.

12.2. Policy

In addition to the provisions under Section 5.4 of this Policy Guideline, the following activities are also strictly prohibited:

- Tampering or manipulating data that would result in falsification/distortion like data inconsistencies or removal of attributions;

- Using the applications to violate laws, rules or regulations, intentionally or unintentionally;

- Providing/Selling data, or copies of the application (whole or in part) to external organizations without written authorization from the data/application owners;

- Transferring software installations/licenses from one device to another without approval from IMS;
- Reverse engineering, decompiling, or disassembling of application without supervision from IMS;
- Modifying the application to bypass implemented security and control measures;
- Incorporating the application (whole or in part) with unsupported applications, to be distributed within or outside the organization; and,
- Using applications to mine data - by way of bots and other methods similar in nature - without approval from IMS.

13. Personally-Owned Devices (PODs)

13.1. Scope

This policy applies to all mobile devices personally-owned by the user that have access to DPWH network, data and systems to store, back up, or relocate any DPWH or user-specific data.

13.2. Expectation of Privacy

PODs will only be accessed by authorized IMS representatives to implement security controls or to respond to legitimate requests as required by administrative, civil or criminal proceedings. On the other hand, users of DPWH-owned IT resources, should have no expectation of privacy while using the equipment and/or services.

The Department shall have the right to remove or delete any files or software installed on these devices that are not compliant with the Department's policies.

13.3. Policy

13.3.1. Access Control

All personally owned mobile devices must be enrolled and approved by the IMS prior to its initial use on the DPWH network or its related infrastructure. The IMS will maintain a list of approved mobile devices and related software applications.

All devices connected to the DPWH network will be monitored by the IMS. The DPWH will not allow devices that are not compliant to the DPWH Technology Architecture or represent a threat to the DPWH network or data.

The IMS shall install and maintain standard configuration of all IT resources including personally-owned laptop/notebook computer connecting to the DPWH network. User shall not install their own software nor change configuration settings without the prior knowledge and consent from the IMS.

13.3.2. Security

All mobile devices must be configured with a lock screen that requires a PIN and/or protected by a strong password. In reference to Section 9.3 of this Policy Guideline, users should never disclose passwords to anyone, even to family members if business work is performed at home.

Likewise, users must employ reasonable security measures to secure their physical device against loss or theft.

To prevent sensitive data from being lost or compromised and to prevent viruses from being spread, users are prohibited from removing security controls on their PODs.

All mobile devices must have:

- up-to-date anti-virus and anti-malware software recommended by the IMS installed on their devices.
- Automatic security updates and other applications update configured to run automatically.

Users are forbidden from copying sensitive data from email, calendar and contact applications to another applications on a device or to an unregistered personally owned device.

Access to Department data is based on user profiles defined by the IMS. Users are required to keep personal data separate from business data on the POD (separate directories), e.g. Private and BYOD to avoid unintentional access to personal information by IT support personnel.

Users must ensure that valuable Department data created or modified on PODs are backed up regularly, preferably by connecting to the DPWH network and synchronizing the data between POD and a network drive, or on a securely stored removable media.

13.3.3. Device Reset and Data Deletion

It is incumbent on the user to report loss or theft of mobile device used for business purposes to the IT Service Desk. The device will be cleared remotely of all data content and locked to prevent access by anyone other than IMS. If the device is recovered, the IMS can perform re-provisioning.

Any device that is to be given, replaced, or discarded must have its permanent data storage wiped. Simple deletion is not enough.

Users must reconcile software licenses purchased by the Department and installed on a personally owned device, and must remove all DPWH data upon separation from the service.

The device will be removed from the DPWH network under the following circumstances:

- non-compliant to this policy;
- device inspection is not granted in accordance with this policy; and,
- user who owns the device no longer has a working relationship with the DPWH.

13.3.4. Liability

DPWH will not reimburse the user the cost of the device and will not pay the cost of data/phone plan in the course of work performed for DPWH.

The Department shall not be liable for the loss or damage of these devices.

13.3.5. Eligibility

DPWH Personnel who require the use of mobile devices to carry out their role in the organization are qualified for mobile access. The personnel's role that fall within the following conditions shall be considered:

a) Mobile – personnel traveling between sites, works from many locations

b) Mobile worker – personnel is oftentimes required to work away from the office.

c) Working from home – personnel needs to work occasionally from home.

d) Emergency use – personnel is required to be available during emergency.

13.3.6. Services and Support

Technical assistance for personally owned devices may be provided only as time permits and if expertise to provide assistance on the device is available.

The IMS shall provide and support baseline connectivity to DPWH email messaging system on personally owned mobile devices with web browser and WIFI connection. The DPWH Outlook Web App (OWA) is accessible on any mobile device including smartphone and tablet computer using internet connections. Refer to Section 11.4 of this Policy Guideline for the guidelines on the use of OWA.

13.4. Request and Agreement Form

A user opting to connect their personal device must complete and sign the "POD Request and Agreement Form" to accept the terms and condition set forth in this policy.

The DPWH reserves the right to authorize or to withdraw the authorization, if deemed appropriate and is in the best interest of the Department, due to the risks associated with Bring Your Own Device (BYOD), such as: loss or corruption of data on POD, malware infection or hacking, non-compliance with existing policies, and violation of intellectual property rights for organization's information created, stored, and processed on PODs.

14. Annexes

14.1. Software and Hardware

14.1.1. Software Request Form

14.1.2. Network Servers Access Request Form

14.1.3. Telephone Line and/or Feature Activation Request Form

14.2. Intranet, Internet and Email

14.2.1. Intranet, Internet and Email Access Request Form

14.3. Application System

14.3.1. CWR User Request Form

14.3.2. MYPS User Request Form

14.3.3. PIS User Request Form

14.3.4. RBIA User Request Form

14.3.5. e-NGAS User Request Form

14.3.6. RTIA Application Request Form

14.3.7. TAS Access Request Form

14.3.8. Data Change Request Form

14.3.9. Request for Information Systems Services

14.3.10. Web Posting Utility Access

Form No. IMS-2014-13-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

REQUEST FOR SOFTWARE

ITSD Incident No. ____________

REQUEST

Employee Name: ______________________

Office/Division/Section: ______________________

Network Account User Name: ______________________

Date of Application: ______________________

Position: ______________________

Contact Number: ______________________

Request For (Please Check)

□ Purchase
□ License Use
□ Installation

Specifications:

____
____
____

(Fill out for License Use and Installation)

Employee Name	Software Name	Version	To be installed on
			□ Desktop □ Laptop □ Server
			□ Desktop □ Laptop □ Server
			□ Desktop □ Laptop □ Server
			□ Desktop □ Laptop □ Server
			□ Desktop □ Laptop □ Server

Purpose:

____
____
____

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: ______________________

Date Completed: ______________________

Action:

□ Approved □ Disapproved

Remarks:

____
____
____

Evaluated by:

____
Chief, Network Administration Section /
Regional IT Support Officer
(Signature over Printed Name)

Recommending Approval:

____
Chief, Technology Support Division
(Signature over Printed Name)

Approved by:

____
Director IV, IMS
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-06-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

NETWORK SERVERS ACCESS
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Date of Application: ____________________

Office/Division/Section: ____________________

Contact Number: ____________________

Server Access:
- □ Shared Folder / Data Repository
- □ Software / System
- □ Others (please specify)

____

Server Machine:
- □ Application Server
- □ Database Server
- □ Web Server
- □ Others (please specify):

Required Server Specifications:

Number of Processor: ____________________

Memory (GB): ____________________

Disk Space (GB): ____________________

Software: ____________________

Staff who will access the server

Name (Lastname, Firstname, MI)	Server/Software/System/Shared Folder Name	Access Rights
		□ View Only □ Full
		□ View Only □ Full
		□ View Only □ Full
		□ View Only □ Full
		□ View Only □ Full

Purpose/s:
- □ File / Data Sharing
- □ For Information / Monitoring
- □ Software / Application Testing
- □ Software / Application Integration
- □ Application Development
- □ Others (Please specify):

____

____

____

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Name of Employee	Signature	Name of Employee	Signature

Attested by:

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: ______________

Date Completed: ______________

Action:

□ Approved □ Disapproved

Remarks:

____

____

Evaluated by:

____
Chief, Systems Administration Section
(Signature over Printed Name)

Recommending Approval:

____
Chief, Technology Support Division
(Signature over Printed Name)

Approved by:

____
Director IV, IMS
(Signature over Printed Name)

Please contact the ITSD for more details about this form

Form No. IMS-2014-04-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

TELEPHONE LINE AND/OR FEATURE ACTIVATION
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Date of Application: ______________________________

Employee Name: ______________________________

Office/Division/Section: ______________________________

Position: ______________________________

Contact Number: ______________________________

Employment Status:

□ Regular Employee

□ Casual / Job Order
(Contract expires on ________________)

□ Consultant / Contractor / Supplier
(Contract expires on ________________)

Average Number of telephone calls:

Nature	Daily	Weekly	Monthly
International			
National (other than DPWH Offices)			
National (DPWH Offices)			

Requested Action: (Please check where applicable)

Type of Access	Purpose / Reason
□ Telephone Line	
□ Telephone Outlet	
□ International Direct Dialing (IDD)	
□ National Direct Dialing (NDD)	

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: ______________ **Date Completed:** ______________

Purpose/s: The Office is (Please check where applicable)

□ involved in disaster, calamity and relief operations
□ involved in research
□ involved in education and training
□ regularly communicating with consultants/contractors
□ regularly communicating with external communities

□ providing results to analysis based on benchmarking against other companies
□ regularly requiring latest information about their profession/functions
□ accomodated in the Department that regularly communicates through telephone with their "Mother" agencies
□ Others (Please specify)______________________________

Action:

□ Approved □ Disapproved

Remarks:

____

Evaluated by:

____
Chief, Network Administration Section /
Regional IT Support Officer
(Signature over Printed Name)

Recommending Approval:

____
Chief, Technology Support Division
(Signature over Printed Name)

Approved by:

____
Director IV, IMS
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-05-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

INTRANET, INTERNET AND EMAIL ACCESS
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Date of Application: ______________________________

Employee Name: ______________________________

Office/Division/Section: ______________________________

Position: ______________________________

Contact Number: ______________________________

Employment Status:

□ Regular Employee

□ Casual / Job Order
(Contract expires on ____________________)

□ Consultant / Contractor / Supplier
(Contract expires on ____________________)

Requested Action: (Please check where applicable)

Type of Access	Purpose / Reason
□ Access Intranet (DPWH website, shared files and printers, etc.)	
□ Access other government websites (GSIS, BIR, DBM, etc.)	
□ Access private organizations' websites (Google, Yahoo, etc.)	
□ Send email to DPWH offices	
□ Send email to other government agencies and private organizations	
□ Increase number of email recipients (default is 10)	
□ Increase email attachment size (default is 10MB)	
□ Increase in mailbox size (default is 250MB)	
□ Delete user account	
□ Disable user account (from: __________ to __________)	
□ Enable user account	

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: ______________ **Date Completed:** ______________

Purpose/s: The Office is (Please check where applicable)

□ involved in disaster, calamity and relief operations
□ involved in research
□ involved in education and training
□ regularly communicating with consultants/contractors
□ regularly communicating with external communities

□ providing results to analysis based on benchmarking against other companies
□ regularly requiring latest information about their profession/functions
□ accomodated in the Department that regularly communicates through email with their "Mother" agencies
□ Others (Please specify)______________________________

Action:

□ Approved □ Disapproved

Remarks:

____

Evaluated by:

____
Chief, Network Administration Section /
Regional IT Support Officer
(Signature over Printed Name)

Recommending Approval:

____
Chief, Technology Support Division
(Signature over Printed Name)

Approved by:

____
Director IV, IMS
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-09-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

CIVIL WORKS REGISTRY (CWR) ACCESS
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Employee Name: ________________________________ Date of Application: ____________________

Office/Division/Section: ________________________________ Position: ____________________

Network Account User Name: ________________________________ Contact Number: ____________________

Request for Access to the following CWR Application and their corresponding User Group Roles:
(Mark only one)

□ Supervisor □ Regional Role

□ Analyst Role □ District Role

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

______________________________ ______________________________
Employee's Signature over Printed Name Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by PrS)

Date Received by PROCUREMENT SERVICE: ____________________

Has the applicant completed the CWR Training course? □ Yes □ No

Action:

□ Approved □ Disapproved

Remarks:

____
____
____

Recommending Approval:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ____________________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-15-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

MULTI YEAR PROGRAMMING AND SCHEDULING APPLICATION (MYPS) ACCESS
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Employee Name: ______________________________ Date of Application: ______________________

Office/Division/Section: ______________________________ Position: ______________________

Network Account User Name: ______________________________ Contact Number: ______________________

Request for Access to the following MYPS Functionality:

RBIA Data Security Group	□ All			□ Others ______________________		
	View	Modify	All		Yes	No
Project Access Rights	□	□	□	Import Work Program	□	□
Program Access Rights	□	□	□	Import CMS Project Data	□	□
Other Work Program Access Rights	□	□	□	Import Road Network	□	□
Road Network Access Rights	□	□	□	Import Other Work Program	□	□
Project Group Access Rights	□	□	□	Modify Options	□	□
				Export Multi Year Program	□	□

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by PS)

Date Received by DEVELOPMENT PLANNING DIVISION, PS: ______________________

Has the applicant completed the MYPS User Training course? □ Yes □ No

Action:

□ Approved □ Disapproved

Remarks:

____

____

____

Recommending Approval:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ______________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-10-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

PERSONAL INFORMATION SYSTEM (PIS) ACCESS
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Employee Name: ______________________________

Date of Application: ______________________________

Office/Division/Section: ______________________________

Position: ______________________________

Network Account User Name: ______________________________

Contact Number: ______________________________

Request for Access to the following PIS Modules and their corresponding User Group Roles:
(Mark only one)

□ Plantilla
- □ Restricted User
- □ Power User
- □ Regional System Administrator

□ Personal Records
- □ Restricted User
- □ Power User
- □ Regional System Administrator

□ Leave
- □ Restricted User
- □ Power User
- □ Regional System Administrator

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by HRAS)

Date Received by HUMAN RESOURCE MANAGEMENT DIVISION, HRAS: ______________________________

Has the applicant completed the PIS Training course? □ Yes □ No

Action:

□ Approved □ Disapproved

Remarks:

____
____
____

Recommending Approval:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ______________________________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-16-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

ROAD AND BRIDGE INFORMATION APPLICATION (RBIA) ACCESS
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Employee Name: ______________________________ Date of Application: ______________________

Office/Division/Section: __________________________ Position: __________________________

Network Account User Name: ________________________ Contact Number: ____________________

Request for Access to the following User and Data Security Groups:

User Group (Mark only one)

□ GIS & LRS
□ Road/Bridge Inventory Configuration
□ Road/Bridge Inventory Update
□ Road/Bridge Condition Configuration
□ Road/Bridge Condition Update
□ Inventory and Condition Update
□ Read Only with Data Sources
□ Read Only
□ Bridge Management System
□ Pavement Management System
□ Routine Maintenance Management System

Data Security Group (Mark only one)

□ All RBIA Data and LRS
□ All RBIA Data and Data Sources
□ All Data (SD Workgroup)
□ All Data (BOM Inventory Workgroup)
□ All Data (BOM Inspectorate Workgroup)
□ Bolt Users
□ Region ____________ (Please specify)

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by PS)

Date Received by STATISTICS DIVISION, PS: ______________________

Has the applicant completed the RBIA User Training course? □ Yes □ No

Action:

□ Approved □ Disapproved

Remarks:

____
____
____

Recommending Approval:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ______________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-08-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

ELECTRONIC NEW GOVERNMENT ACCOUNTING SYSTEM (e-NGAS) ACCESS
REQUEST FORM

ITSD Incident No. ____________

REQUEST

Employee Name: ______________________________

Office/Division/Section: ______________________________

Network Account User Name: ______________________________

Date of Application: ______________________________

Position: ______________________________

Contact Number: ______________________________

Request for Access to the following e-NGAS Modules and their corresponding User Group Roles:
(Mark only one)

Modules:

□ Accounting

□ eBudget

User Group Roles:

□ Preparation

□ Approval

□ Audit / Read Only

□ IT Support Officer

□ System Administrator

□ Data Steward / AUC

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by FMS)

Date Received by ACCOUNTING DIVISION, FMS: ____________________

Has the applicant completed the e-NGAS Training course? □ Yes □ No

Action:

□ Approved □ Disapproved

Remarks:

____

____

____

Recommending Approval:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ____________________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

ROAD TRAFFIC INFORMATION APPLICATION (RTIA) ACCESS
REQUEST FORM

ITSD Incident No. ____________

REQUEST

Employee Name: ____________________ Date of Application: ____________

Office/Division/Section: ____________________ Position: ____________

Network Account User Name: ____________________ Contact Number: ____________

Request for Access to the following RTIA Modules:

Survey Site Hierarchy
- □ Modify
- □ Delete

Axle Load Section
- □ Insert
- □ Modify
- □ Delete

NRTSP
- □ Modify

Equipment
- □ Insert
- □ Modify
- □ Delete

LRS Road Section & LRP
- □ Import

Traffic Section
- □ Insert
- □ Modify
- □ Delete

Seasonal Factor
- □ Modify

Non-NRTSP Survey
- □ Insert
- □ Modify
- □ Delete

Summary Data
- □ Generate

Quality Assurance
- □ Approve

□ Run TDE Application

Regional Access: ____________

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by BQS)

Date Received by TRAFFIC ENGINEERING DIVISION, BQS: ____________________

Has the applicant completed the RTIA User Training course? □ Yes □ No

Action:

□ Approved □ Disapproved

Remarks:

____

____

____

Recommending Approval:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ____________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-11-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

TIME AND ATTENDANCE SYSTEM (TAS) ACCESS
REQUEST FORM

ITSD Incident No. ____________

REQUEST

Employee Name: ______________________________

Date of Application: ____________________

Office/Division/Section: ______________________________

Position: ____________________

Network Account User Name: ______________________________

Contact Number: ____________________

Request for Access to the following TAS Modules and their corresponding User Group Roles:
(Mark only one)

□ Administrator

□ Primary TAS Officer

□ Alternate TAS Officer

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources, Department Order No. 013, series 2015, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT Resources and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

EVALUATION OF REQUEST (to be filled out by HRAS)

Date Received by HUMAN RESOURCE MANAGEMENT DIVISION, HRAS: ____________________

Has the applicant completed the TAS Training course? □ Yes □ No

Action:

□ Approved □ Disapproved

Remarks:

____

____

____

Recommending Approval:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ____________________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-07-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

DATA CHANGE
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Date of Application: ______________________________

Office/Division/Section: ______________________________

Name of Application System: ______________________________

Record ID	Description	Request to		Reason / Correction
		Delete	Edit	

Requested by:

____
Application User Coordinator
(Signature over Printed Name)

Approved by:

____
Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Action:

□ Approved □ Disapproved

Remarks:

____

____

____

Recommending Approval:

____
Chief, Application Support Division
(Signature over Printed Name)

Approved by:

____
Director IV, IMS
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Form No. IMS-2014-12-00

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

REQUEST FOR INFORMATION SYSTEMS SERVICES

ITSD Incident No. ____________

REQUEST (to be filled out by the AUC)

Date Requested: ______________________

Date Required: ______________________

Requesting Office: ______________________

Contact Number: ______________________

Name of Application: ______________________

Type of Service requested:

□ Development (New Application)

□ Enhancement (Reports, Additional Functionalities / Modules)

Please provide a detailed description of the request. Attach additional documents as necessary.

Note:

For requests involving reports, please attach a sample format of the report (may contain data). The format must be initiated by the AUC and Head of Office. IMS will not process the request if a sample report is not provided.

□ Sample format attached

Requested by:

____
Application User Coordinator
(Signature Over Printed Name)

Approved by:

____
Head of Office
(Signature Over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Assigned ASP: ______________________
(Signature over Printed Name)

Date Received by ASP: ______________________

Action:

□ Approved

□ Disapproved

□ Deferred

Remarks:

____

____

____

Recommending Approval:

____
Chief, Application Support Division
(Signature over Printed Name)

Approved by:

____
Director IV, IMS
(Signature over Printed Name)

Please contact the ITSD for more details about this form.

Department of Public Works and Highways
IT SERVICE DESK
Information Management Service
ICC Building, Bonifacio Drive, Port Area, Manila

WEB POSTING UTILITY ACCESS
REQUEST FORM

ITSD Incident No. ______________

REQUEST

Employee Name: ______________________________ Date of Application: ______________________

Office/Division/Section: ______________________________ Position: ______________________

E-mail Address: ______________________________ Contact Number: ______________________

Request for Access to the following Web Posting Utility Modules:
(Please check)

□ Civil Works

□ Consultancy

□ Goods

□ Program of Works

□ Realignment

□ LDDAP - ADA

Requested / Authorized by:

____
Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Department Order No. 045, series 2012 - Update, Maintenance, and Quality Assurance of the DPWH Website, and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the Web Posting Utility Tools and/or be subjected to disciplinary actions.

Attested by:

____
Employee's Signature over Printed Name

____
Supervisor's Signature over Printed Name

ACCESS GRANTING (to be filled out by IMS)

User Privileges Implemented on Date: ______________

Implemented by:

____
Application Support Person
(Signature over Printed Name)

Please contact the ITSD for more details about this form.