

Republic of the Philippines DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS OFFICE OF THE SECRETARY

Manila



JAN 2 1 2025

DEPARTMENT ORDER)
	00)
	()Q)
NO	00)
Serie	s of 2025		
	d	1/22/20	25

SUBJECT: Policies and Guidelines on the Use of Information **DPWH** 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 that the policies and guidelines on the proper utilization of these resources are aligned with cybersecurity best practices and current trends and developments in technology, the attached updated 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 shall supersede Department Order No. 58, Series of 2024 and shall take effect immediately.

MANUEL M. BONOAN Secretary

11.1.2 RGG/RBC

WIN5P01856

Website: https://www.dpwh.gov.ph Tel. No(s).: 5304-3000 / (02) 165-02



Bonifacio Drive, Port Area, Manila

Policies and Guidelines on the Use of

DPWH

Information and Communications Technology (ICT) Resources

Revision No. 03

Table of Contents

Acr	onyms		. 4
1.	Purpose		. 5
2.	Scope		. 5
3.	Definition	on of Terms	. 5
4.	Duties a	nd Responsibilities	. 7
	4.1.	All Users	. 7
	4.2.	Division and Section Chiefs	. 7
	4.3. Officers	Information Management Service (IMS) and Regional/District IT Support	
	4.4.	IT Service Desk	8
5.	General	Policy	8
	5.1.	Acceptable Use of ICT Resources	8
	5.2.	Request for Access and Approval	9
		5.2.1 Request for Access	9
		5.2.2 Approval	9
		5.2.3 Access Review	9
	5.3.	Monitoring of Compliance	.0
	5.4.	Data Security and Accountability	0.
	5.5.	Revocation of Privileges 1	.0
	5.6.	Sanctions 1	.1
6.	ICT Equ	ipment 1	.1
7.	Software	e and Licenses1	.2
8.	Telepho	ne Service1	.3
9.	Intranet	Service 1	3
	9.1.	Network Account1	3
	9.2.	Confidentiality and Security	3
	9.3.	Account Lockout 1	4
	9.4.	Temporary Deactivation of Network Account 1	4
10.	Internet	Service	4
11.	VPN Acc	ess Service	5
12.	Email Se	rvice1	6
13.	File Stor	age Service1	7
14.	Applicati	on Systems1	7
15.	Personal	ly-Owned Devices (PODs)1	8
	15 1	Manitoring of Compliance	0

	15.2.	Access	Control 18	8
	15.3.	Security	/	8
	15.4.	Device	Reset and Data Deletion19	9
	15.5.	Liability		9
	15.6.	Service	s and Support19	9
	15.7.	Revoca	tion of Access19	9
16.	General	Guidelin	es20)
	16.1.	Reques	t for Access to the Department's ICT Services20)
	16.2.	Reques	t for Access to the Department's Application Systems22	2
		22		
	16.3.	Reques	t for VPN Access23	3
	16.4.	Accessii	ng Email Platforms24	1
		16.4.1.	Standard Email	1
		16.4.2.	Microsoft Office 365 Email25	5
		16.4.3.	Email Capacity Limits25	5
	16.5.	Exchang	ging Large Files25	5
		16.5.1.	DPWH FileDrop25	5
		16.5.2.	OneDrive for Office 365 Users	5
		16.5.3.	SharePoint	5
17.	Annexes	S		;
	17.1.	Software	e and Hardware26	;
		17.1.1.	File Servers Access Request Form	;
		17.1.2.	Personally-Owned Device (POD) Configuration Request Form 26	,
		17.1.3.	Software Request Form26	;
		17.1.4.	Telephone Line and/or Feature Activation Request Form 26	j
		17.1.5.	VPN Access Request Form	į
	17.2.	Intranet	, Internet, and Email26	,
		17.2.1.	Intranet Access Request Form	,
		17.2.2.	Internet and Email Access Request Form26	,
		17.2.3.	Change of Network Account Request Form26	,
	17.3.	Applicati	on System26	,
		17.3.1.	CEA Access Request Form26	
		17.3.2.	CuSSA Access Request Form 26	
		17.3.3.	CWA Access Request Form26	
		17.3.4.	DMA Access Request Form	
		17.3.5.	DoTS Access Request Form	

17.3.6.	eBudget Access Request Form	26
17.3.7.	eNGAS Access Request Form	26
17.3.8.	IROWMA Access Request Form	26
17.3.9.	MYPS Access Request Form	26
17.3.10.	PCMA Access Request Form	26
17.3.11.	PIS Access Request Form	26
17.3.12.	PPMPA Access Request Form	26
17.3.13.	RBIA Access Request Form	26
17.3.14.	RPS Access Request Form	26
17.3.15.	RTIA Access Request Form	27
17.3.16.	TAS Access Request Form	27
17.3.17.	Web Posting Utility Access Request Form	27
17.3.18.	Data Change Request Form	27
17.3.19.	Request for Information Systems Services	27

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
VPN	Virtual Private Network
WFH	Work From Home

1. Purpose

The appropriate and legitimate use of Information and Communications Technology (ICT) resources is a vital concern for an organization. The purpose of this document is to define the policies and guidelines for authorized users to use or access the Department's ICT resources.

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

2. Scope

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

3. Definition of Terms

Application System	A system to which a computer program	or software is applied,
--------------------	--------------------------------------	-------------------------

such as Civil Works Application (CWA) and Document Tracking

System (DoTS).

Bring your own device

(BYOD)

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

Cyber Threat Any circumstance or event with the potential to adversely

impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information,

and/or denial of service.

Freeware Software that is available to the users, free of cost to use and

distribute. The source code of the software is not available to

use and cannot be modified.

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.

Hardware All equipment involved in the operations of a computer

system, which includes, but is not limited to, computers, mobile devices, data communications equipment, workstations, and various peripherals such as printers and

plotters.

Information and Communications 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.

Intranet

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

Network ID

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

Mobile devices

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

Multi-factor Authentication (MFA)

A security mechanism that requires users to provide two or more forms of authentication before they can access an account, system, or service (e.g., password and a code sent to a mobile device).

Peripherals

Any external devices connected to a computer.

Personally-owned device (POD)

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

Phishing

A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

Shareware

Software that is initially available to the users free of cost to use and distribute, but after some time, the software is required to be paid. The source code of the software is not available to use and cannot be modified.

Software

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

Spoofing

Faking the sending address of a transmission to gain illegal entry into a secure system.

Virtual Private Network (VPN)

A service that establishes a secure connection between a computing device and a computer network or between two networks.

Work-from-home (WFH) A work arrangement where government officials or employees

work at home or their residence.

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 runs multi-

user operating systems.

4. Duties and Responsibilities

4.1. All Users

All users shall adhere to the policies and guidelines prescribed herein. Failure to do so may lead to revocation of privileges and/or disciplinary action as provided under Sections 5.5 and 5.6. of this Policy Guideline.

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 backup of their files on workstations. Users are also responsible for reporting ICT--related problems to the IT Service Desk.

Users who work on non-Department-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 5.4 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 these resources are utilized for their intended purpose. They shall report any violation of this Policy Guideline to the IMS.

Supervisors should ensure that new employees are given orientation on this Policy Guideline 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 (RITSO/DITSO)

IMS shall set the rules and regulations for the installation of duly authorized and approved hardware, software, and other peripherals owned by the Department, including the

maintenance and security of data and network equipment, and formulation and implementation of an ICT disaster recovery plan.

IMS and the RITSO/DITSO shall remove all unauthorized hardware and/or software connected to/installed in the Department's ICT Infrastructure and recommend sanctions to erring employees as provided under Section 5.6 of this Policy Guideline.

IMS and the RITSO/DITSO 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 RITSO/DITSO shall only maintain telephones/fax machines connected to the communication network.

IMS and the RITSO/DITSO shall only maintain and provide security for the Department's centralized internet connection and email system. They will not be liable for any security breach/threats from using portable or wired broadband internet connection 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 through its hotline number 43070 (external number 5304-3070), through email at itservicedesk@dpwh.gov.ph, or the DPWH IT Service Desk Customer Portal accessible on the DPWH Intranet Website.

5. General Policy

5.1. Acceptable Use of ICT Resources

The DPWH ICT resources are intended to support the Department's legitimate business requirements. Employees are expected to use the Department's ICT resources in a responsible, professional and lawful manner.

The DPWH ICT resources should not be used for any purpose that could damage the Department's institutional image and/or strain its operational efficiency or compromise its security and integrity. Thus, the following are strictly prohibited:

- saving/sharing offensive content of any kind, including pornographic materials;
- promoting discrimination on the basis of race, sex, age, gender, religion, disability, social status, etc.;
- exhibiting harassment, threats, or violent behavior;
- gambling, theft, piracy, and other illegal/fraudulent activities;
- obtaining personal financial gain;
- engaging activities that reduce the productivity of users;
- system hacking or deliberately propagating computer viruses, malwares, and other cyber threats:
- accessing and/or dispensing confidential data/information without authorization;
- unauthorized access to, use of, or tampering of the ICT resources;

- unauthorized accessing of DPWH data or files of other employees;
- using the network ID of other employees;
- unauthorized broadcasting of bulk messages to all users;
- sharing or transferring of large files across the network that are not relevant to the business operations of the Department, and,
- any activity that violates any government law, code, or Policy.

Occasional and reasonable use of the DPWH ICT resources for personal purposes is regarded as acceptable, provided that:

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

5.2. Request for Access and Approval

5.2.1 Request for Access

Requests for access to the DPWH ICT resources shall be approved only if reasonable business needs are identified and shall be granted based on the individual's job responsibilities, as attested by the immediate Supervisor, which involves, but is not limited to, the following:

- research, procurement, public information, education, and training;
- infrastructure planning, design, and construction;
- 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.

The duly accomplished access request form shall be submitted to signify that the requesting party understands and agrees to comply with all relevant DPWH ICT policies.

5.2.2 Approval

The access request form should be signed by the users' immediate Supervisor and Head of Office and submitted to the IT Service Desk for processing.

For access to application systems, the requesting office must submit the duly accomplished request form to the appropriate Application User Coordinator (AUC) for evaluation prior to submission to the IT Service Desk.

5.2.3 Access Review

User access privileges shall be reviewed on a regular basis to ensure users have only the minimum access required for their job functions. The following user access review shall be implemented by the concerned offices with the assistance of the IMS:

User Access	Responsible Office	Frequency	
Standard user access	IMS	Every 4 th week of January	
Privilege accounts	IMS	Every 1st week of June and December	
Application user access	Application User Coordinator	Every 4 th week of January	
Shared folder access	Shared Folder Owner	Every 4 th week of January	
Email access	Concerned Office	Every 4 th week of January	
Third-party access (consultants, vendors, etc.)	Concerned Office	Every 1st week of June and December	

The IMS shall maintain the users access inventory of the abovementioned systems.

5.3. Monitoring of Compliance

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

The Department 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 a condition of use, that such facilities, whether used for official business or personal purposes, will be monitored.

5.4. Data Security and Accountability

The use, management, and protection of the Department's data shall be in accordance with the most current Policy on the Implementation of a Data Governance Program.

5.5. Revocation of Privileges

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

In case of a 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.

Email accounts that have been inactive for sixty (60) calendar days without prior notice to the IMS shall be marked for revocation. The IMS shall notify the concerned Head of Office regarding the revocation of dormant or inactive email accounts.

The Department reserves the right to revoke users' ICT privileges for any violation of this Policy Guideline at any time and without prior notice and to impose sanctions stipulated in Section 5.6.

5.6. 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. ICT Equipment

This Policy applies to all Department-owned or leased ICT equipment, including installed physical components, accessories, parts, or peripherals.

All servers, desktop and laptop computers, and network printers should be configured with the standard configuration issued by the IMS. The standard configuration for desktop and laptop computers shall include, but are not limited to, the following:

- Installed with an Operating System compatible with the Department's Active Directory Domain System;
- Installed with standard tools and authorized software and application systems;
- Installed with an updated endpoint security software;
- Configured with standard computer naming convention;
- Connected to the DPWH communication network;
- Joined/configured to the Active Directory Domain Service;
- Password-protected BIOS:
- Restricted access for regular users;
- Disabled local administrator and guest accounts; and,
- Configured with the standard local administrator account with a strong password.

All Department-owned computers running on Windows Operating Systems that are no longer supported (end-of-life) by Microsoft and endpoint security manufacturers should not be connected to the Department's communication network and should be decommissioned immediately as these are vulnerable to cybersecurity risks.

Only IMS personnel and Regional/District IT Support Officers are authorized to configure and connect ICT equipment to the Department's communications network and perform all types of equipment (including network ports and cables) installations, disconnections, modifications, and relocations.

All newly procured or turned-over equipment shall be endorsed to the IT Service Desk or concerned IT Support Officers for inspection, proper configuration, and inventory in compliance with the most current Guidelines on the Procurement, Turn-Over, Inspection, Disposal and Inventory of ICT Resources.

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.

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

ICT 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 Supervisor knows what equipment is being taken out, what data is on it, and for what purpose it will be used. Equipment that has been taken out of the office should be brought back upon returning to the office.

7. Software and Licenses

This Policy applies to all Department-owned or subscribed applications or software, whether commercial, in-house developed, or open source.

Only software authorized by the IMS and those that are licensed to or owned by the Department are to be installed on the Department's computers. Only IMS personnel and Regional/District IT Support Officers are authorized to download, copy, and install software and applications to the Department's equipment.

Users are prohibited from downloading, copying, installing, and using the following non-standard software:

- unauthorized/unlicensed proprietary/commercial software
- unauthorized freeware/shareware
- free for personal use software
- trial software with an existing license owned by the Department
- cracked or pirated software
- personally-owned software
- software licensed to other organizations or institutions (except for those with authorization from the license owner and the manufacturer)

All software installations must comply with applicable licensing agreements, including the number of permitted installations and terms of use, and shall adhere to all the laws and regulations regarding copyright and Intellectual Property Rights (IPR).

All software (package, programs, or applications), data, and data files loaded on the Department's computer are properties of the Department. As such, the Department retains the right to access, copy, change, alter, modify, destroy, delete, or erase any of these from the Department's computers.

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

8. Telephone Service

This Policy applies to all Department-owned or leased telephone equipment connected to the Department's communications network.

The telephone service shall be used for official business purposes only. Personal calls should be kept to a minimum and limited to emergencies or essential situations.

A professional and courteous demeanor should always be maintained during phone conversations, and proper telephone etiquette should be observed at all times.

Users must respect the confidentiality of sensitive information discussed over the phone and take appropriate measures to ensure privacy.

International and long-distance calls should be made only when necessary and approved by the Supervisor.

The telephone service should not be tampered with to gain access to other features and should not be used for:

- auto-dialing, continuous or extensive call forwarding, or connecting to any device that permits the services to be used as an outbound trunk by more than one individual;
- forwarding calls from an external number to any DPWH local number or vice versa; and,
- telemarketing or fax broadcasting.

9. Intranet Service

The Intranet service that enables access to ICT resources, which includes the telephone system, websites, applications, internet, email, data, and other shared resources, is provided to facilitate efficient internal communications and collaboration.

9.1. Network Account

Upon approval of the access request form, the user shall be given a Network ID to access the intranet and other DPWH ICT resources. The users are responsible and accountable for all activities carried out under their Network ID. The standard DPWH Network ID is a combination of the user's last name, the first letter of the first name, and the first letter of the middle name.

9.2. Confidentiality and Security

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.

Network 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 Network ID and password.

The users must adhere to the following minimum complexity requirements in creating strong passwords:

- Must be at least sixteen (16) characters;
- Must be a combination of uppercase and lowercase letters, numbers and special characters;
- Must be different from the Network ID and NOT an anagram of it; and,
- Must not include obvious and easy-to-guess words such as password, abcd1234, dpwh2023, and the like.

The system automatically notifies users to change their password every three hundred sixty-five (365) calendar days. In the event of an expired password, the user shall request a password reset through the IT Service Desk. If access is required in the absence of the user, a written consent signed by the user's Supervisor or Head of Office must be presented to the IMS.

To reduce the risk of unauthorized access, multifactor authentication (MFA) shall be implemented for users who have access to the following:

- Microsoft Office 365 (Outlook, SharePoint, Teams, Forms, etc.)
- Virtual Private Network (VPN)
- Internet-facing web applications (NGOBIA, EDMS, etc.)

9.3. Account Lockout

For security, the Network Account will be locked out after five (5) invalid login 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 Network Account 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 Network Account

A user who will be away from the office for more than two (2) months and does not intend to access his/her Network Account may request its temporary deactivation to ensure that no one will be able to use the user's Network Account while they are away.

10. Internet Service

This Policy applies to all internet services under the jurisdiction and/or ownership of the Department that are being accessed on any computers or devices, whether these are connected to the Department's communications network or stand-alone workstations.

Computers equipped with both wired and wireless network connections should not be simultaneously connected to third-party internet connection and the Department's communications network to avoid security risks as this may pose a potential backdoor or avenue for hackers to infiltrate our network.

Servers should not be connected to the internet unless necessary and authorized by the IMS.

Except if being used for official purposes and with approval by IMS, the use of the internet service for the following activities is strictly prohibited:

- Accessing sites that may compromise the security of the Department's communications network, e.g., external webmail, 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.;
- Downloading of files that may introduce viruses or malwares, e.g., pirated software, shareware, freeware, torrents, etc.; and,
- Activities that may put unnecessary strain on the internet bandwidth, e.g., downloading large files, file sharing sites, video streaming, etc.

Access to Facebook and Messenger will be restricted, except for Stakeholders Relations Service (SRS) personnel and Public Information Officers as authorized by their respective Heads of Offices. These platforms shall be accessible to the general internet users of the Department from 11:00 am to 1:00 pm only.

11. VPN Access Service

Virtual Private Network (VPN) access is provided to enable users with legitimate business needs to connect securely to the Department's communications network from remote locations.

VPN access shall be available only within the Philippines. Users traveling outside the country who need to use VPN access should notify IMS in advance through the IT Service Desk.

Only the VPN client/software authorized by the IMS shall be used for remote access and shall only be installed on computers owned by the Department. It should never be used on non-Department-owned computers.

It is the responsibility of the users with VPN privileges to ensure that their account or device are not being used by unauthorized individuals to access the Department's communications network. They should also employ reasonable security measures to secure their physical device against loss or theft.

VPN privileges shall be deactivated once the user fails to utilize the service for more than three (3) months. Users will be notified in advance prior to deactivation of their VPN access.

Computers that are being used for VPN access should be secured and installed with an updated endpoint security software authorized by the IMS. The user is responsible for ensuring that the virus definition of the said endpoint security software is up-to-date.

These computers should be brought to the IT Service Desk or concerned IT Support Officers on a monthly basis for cyber threat assessment and checking.

12. Email Service

This Policy applies to all email services under the ownership and/or subscription of the Department, including all its associated emails stored on the user's devices.

The Department prescribes the use of its official email (@dpwh.gov.ph) in communicating and transacting official business with other entities to establish and maintain its corporate identity. All employees are prohibited from using their personal or unofficial emails for official business transactions of the Department. Consequently, the use of free for personal use web-based email, such as Gmail or Yahoo Mail, shall be prohibited within the Department's communication network.

Since users carry the name of DPWH each time they use official ICT channels of communication, prudence must be diligently observed. When using official ICT channels, users expressing personal opinions or taking a personal stand on issues must explicitly state that what they expressed does not represent DPWH.

Users are obliged to use this service in a responsible and lawful manner, and are strictly prohibited from:

- forwarding or sending and/or storing emails and other files of inappropriate and/or illegal contents;
- disclosing confidential information and personal data that violates the Data Privacy Act and its Implementing Rules and Regulations;
- forwarding or sending files containing viruses, spams and other malicious files;
- using official email for promotion or campaign during elections and other partisan activities; and,
- using official email to subscribe to any website that is not relevant to one's work or the Department's operations.

All messages distributed using the Department's email service are property of the Department, thus, it has the right, without prior notification, to monitor, access/view, retrieve, delete, and disclose user's emails if deemed necessary.

Emails that contain confidential or sensitive data should be sent or forwarded to the intended recipients only.

Users shall adopt the following security measures to minimize the threat of cyber attacks such as phishing, spoofing, or scams:

- Attachments or links from unsolicited emails coming from unknown senders should not be opened;
- Email contents should be checked for common signs of phishing or scam, such as:
 - o requesting for personal and/or financial information;
 - o grammar and spelling errors;
 - o sense of urgency or unusual requests;
 - o inconsistencies in the email address and links; and
 - o contains threats on the alleged recorded malicious activity of the user.
- Suspicious emails should be reported immediately to the IT Service Desk.

To reduce the risk of unauthorized access, multifactor authentication (MFA) shall be implemented for Microsoft Office 365 users.

13. File Storage Service

File storage or shared folders are provided to offices that require a central repository of electronic files or documents that are being used for office collaboration, as a reference for a business process, or as a component of an enterprise application system.

Only the users authorized by the concerned Head of Office shall be given access (read-only or full access) to their office file storage folders. It is the responsibility of these users to ensure that their account or device are not being used by unauthorized individuals to access their files.

Users with privileged access to the file storage shall not be allowed to share the files from the storage with other individuals without consent from the Head of Office or immediate Supervisor.

The concerned office (owner of the file storage folder) shall be responsible for ensuring that the files being uploaded by their employees are legitimate official documents of the Department. Uploading of employee's personal files is prohibited.

The concerned office shall be responsible for ensuring that they adhere to all the provisions of the Department's Data Governance Program, Data Privacy Act and its Implementing Rules and Regulations, and other relevant policies on file sharing.

14. Application Systems

This Policy applies to 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.

Users are obliged to use these systems in a responsible and lawful manner and are strictly prohibited from:

- 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 similar methods without approval from IMS.

15. Personally-Owned Devices (PODs)

This Policy applies to all devices personally-owned by the employees that are being used for the conduct of their official duties and tasks and have access to the Department's ICT resources.

15.1. Monitoring of Compliance

Users of the DPWH ICT resources, regardless of the equipment (PODs or Department-owned) and/or services they are using, shall be monitored for compliance with all relevant policies and guideline of the Department.

PODs will only be accessed by authorized IMS representatives to configure security controls or to respond to legitimate requests as required by administrative, civil, or criminal proceedings.

It is understood that when using PODs, the user agrees that 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.

15.2. Access Control

All personally-owned devices must be enrolled and approved by the IMS prior to their initial use on the Department's communications network or its related infrastructure.

The IMS will monitor all devices connected to the Department's communications network. Additionally, any devices that are not compliant with the DPWH Standards for ICT Equipment and/or deemed vulnerable to cybersecurity threats, which could compromise the Department's communications network or data, shall also be prohibited.

The IMS shall install and maintain standard configuration of all personally-owned laptop/notebook computers that have been authorized to connect to the Department's communications network. Users shall not install their own software nor change configuration settings without prior knowledge and consent from the IMS. Department-owned software should not be installed to these computers.

Authorized mobile devices, either DPWH-owned or PODs, should not be connected to the Department's intranet. These devices should only be connected on an isolated or separate network that has internet access.

15.3. Security

All devices must be configured with a lock screen that requires a PIN and/or protected by a strong password. 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 devices 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 personally-owned devices must have the following:

- Up-to-date anti-virus and anti-malware software recommended by the IMS installed on their devices.
- · Security and application updates configured to run automatically.

Users are prohibited from copying sensitive data to an unregistered, personally-owned device.

Access to Department data is based on user profiles defined by the IMS. Users are advised to keep personal data separate from business data on the POD 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.

15.4. Device Reset and Data Deletion

It is incumbent on the user to report the loss or theft of a 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.

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 Department's communications network under the following circumstances:

- non-compliant with this Policy;
- device inspection is not granted in accordance with this Policy; and,
- users who own the device no longer have a working relationship with the DPWH.

15.5. Liability

The Department will not reimburse the user the cost of the device and will not pay the cost of the 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.

15.6. Services and Support

The IMS shall provide and support baseline connectivity to the Department's email system on personally-owned mobile devices with a web browser and WIFI connection. The Microsoft Outlook Web App (OWA) and Office 365 are accessible on any mobile device with an internet connection.

15.7. Revocation of Access

The Department reserves the right to revoke access to the DPWH ICT resources using PODs due to the following:

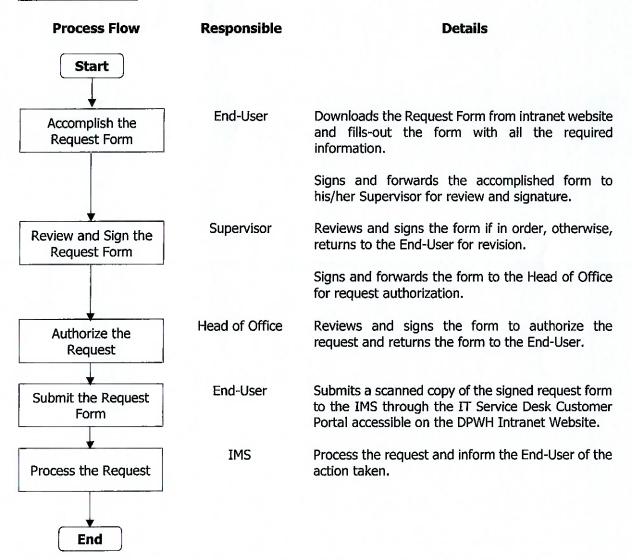
- malware infection or hacking;
- violation of intellectual property rights for the organization's information created, stored, and processed on PODs; and,
- non-compliance with this Policy Guideline.

16. General Guidelines

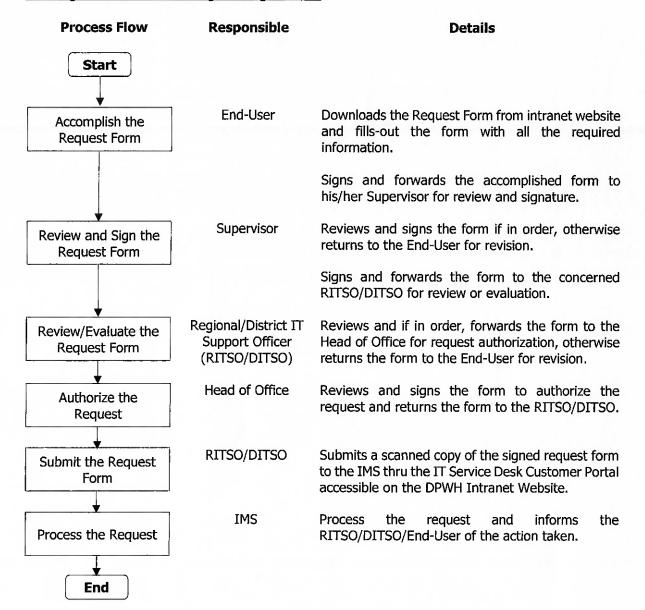
16.1. Request for Access to the Department's ICT Services

Employees and officials with legitimate business needs may request access to the Department's ICT services by submitting the appropriate duly accomplished request form, which are downloadable from the intranet website (http://dpwhweb/downloads/index.htm). The following procedures shall be followed for requesting access to the Department's ICT services:

For Central Office:

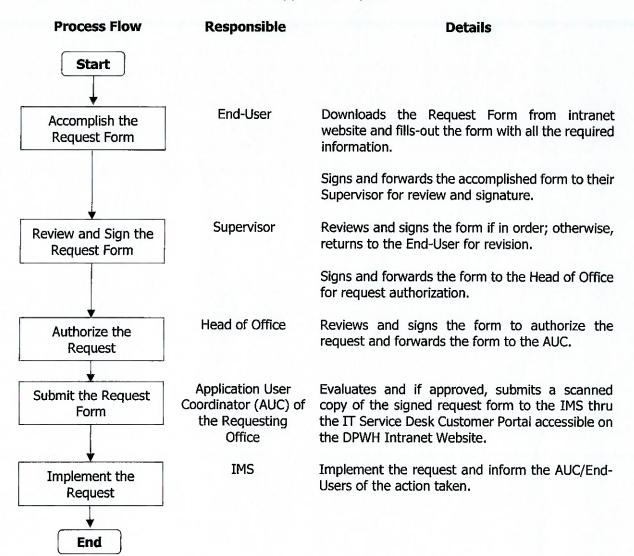


For Regional and District Engineering Offices:



16.2. Request for Access to the Department's Application Systems

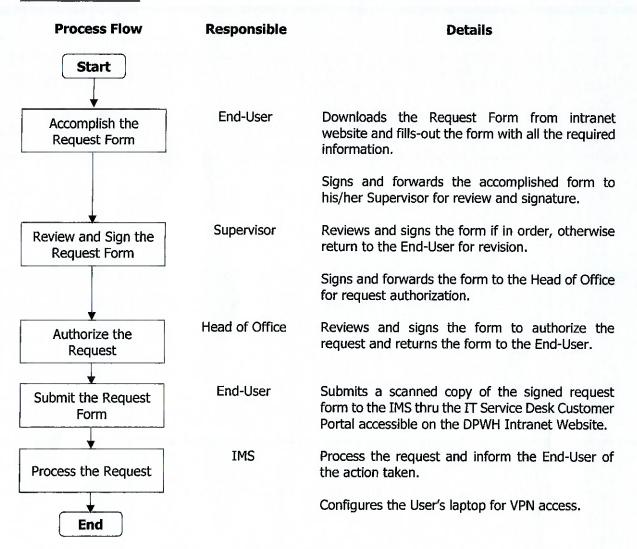
Employees and officials with legitimate business needs may request access to the Department's Application Systems by submitting the appropriate duly accomplished request form, which are downloadable from the intranet website (http://dpwhweb/downloads/index.htm). The following procedures shall be followed for requesting access to the Department's Application Systems:



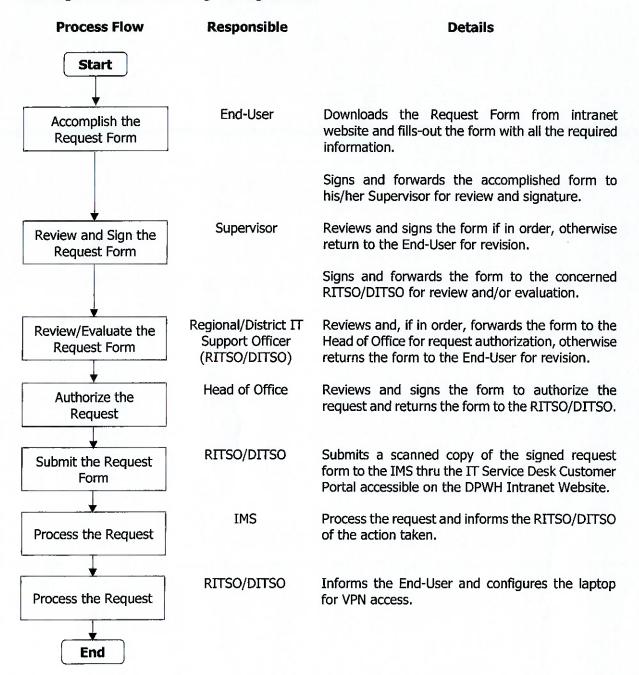
16.3. Request for VPN Access

Employees (with DPWH-issued laptop computers) who require remote access to the Department's network may request VPN access by submitting a duly accomplished VPN Access Request Form, which is downloadable from the intranet website. The following procedures shall be followed for requesting VPN access:

For Central Office:



For Regional and District Engineering Offices:



16.4. Accessing Email Platforms

16.4.1. Standard Email

The Department is using Microsoft Exchange Server for its standard email system, which is hosted on-premise. The email system is accessible using the following:

a. Microsoft Outlook for Desktop and Mobile Devices

Microsoft Outlook is an email client that is pre-installed on the Department's standard desktops and laptops as part of the Microsoft Office Standard suite. It can also be downloaded on mobile devices from Google Play Store and Apple App Store.

Employees with approved email access may request the configuration of their Microsoft Outlook from the IT Service Desk or the concerned IT Support Officers.

b. Outlook Web App (OWA)

OWA is the web-based version of the Department's standard email system, which is accessible internally through the Department's communication network and externally via a commercial internet connection. It can be accessed on web browsers like Microsoft Edge, Mozilla Firefox, or Google Chrome using the link: 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 network ID and password; and,
- always log out from OWA and close browser sessions when done.

16.4.2. Microsoft Office 365 Email

Microsoft Office 365 is a cloud-based productivity platform that comes with various apps, video conferencing, storage, and email system, which are accessible via internet connection. The Office 365 Email can be accessed on web browsers like Microsoft Edge, Mozilla Firefox, or Google Chrome using the link: https://outlook.office.com/owa/.

Microsoft Outlook (desktop and mobile app) may also be used for accessing the Office 365 email.

16 12	Empil	Capacity	Limita
10.4.3.	LHIAH	Capacity	LIIIIILS

Features	Standard Email	Office 365 Email
Mailbox capacity	500 MB	50,000 MB
Maximum number of email recipients	20 recipients	5,000 recipients
Email attachment size limit	30 MB	30 MB for non-Office 365 recipients
	Note: this is the standard limit of the majority of the email providers	150 MB for Office 365 recipients

16.5. Exchanging Large Files

16.5.1. DPWH FileDrop

DPWH FileDrop is a web application that allows users to easily and securely share files within the Department's communications network by uploading the files into the web application and sending the download link or QR code to the intended recipient.

It can be accessed using any web browser like Microsoft Edge, Mozilla Firefox, or Google Chrome through the link: http://filedrop.dpwh.gov.ph.

Files uploaded to the DPWH FileDrop are automatically deleted after seven (7) days (by default) or the retention period set by the sender.

The DPWH FileDrop is available or accessible only within the Department's communications network.

16.5.2. OneDrive for Office 365 Users

Another way to send large files for Office 365 users is OneDrive. OneDrive is an Office 365 application that allows users to store files in the cloud. Stored files can be shared by giving access to other users.

16.5.3. SharePoint

SharePoint is a browser-based collaboration and document management platform that allows users to share files with a single user or with groups. As this is also a cloud-based storage, two or more users can work on the same document simultaneously.

17. Annexes

17.1. Software and Hardware

- File Servers Access Request Form
- Personally-Owned Device (POD) Configuration Request Form
- Software Request Form
- Telephone Line and/or Feature Activation Request Form
- VPN Access Request Form

17.2. Intranet, Internet, and Email

- Intranet Access Request Form
- Internet and Email Access Request Form
- Change of Network Account Request Form

17.3. Application System

- CEA Access Request Form
- CuSSA Access Request Form
- CWA Access Request Form
- DMA Access Request Form
- DoTS Access Request Form
- eBudget Access Request Form
- eNGAS Access Request Form
- IROWMA Access Request Form
- MYPS Access Request Form
- PCMA Access Request Form
- PIS Access Request Form
- PPMPA Access Request Form
- RBIA Access Request Form
- RPS Access Request Form

D.O. No. **(A)** Series of 2025 Policies and Guidelines on the Use of DPWH ICT Resources Page 27 of 27

- RTIA Access Request Form
 TAS Access Request Form
 Web Posting Utility Access Request Form
 Data Change Request Form
- Request for Information Systems Services



Republic of the Philippines DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS **CENTRAL OFFICE** Bonifacio Drive, Port Area, Manila

FILE SERVER ACCESS REQUEST FORM

	REQUEST	Service Request No.			
Date of Application:		Shared Folder N	Name:		
Office:					
	(Office, Division, Section)				
Name of Employee	Subfolder Name (e.g. \S	Shared Folder\Subfolder\)	Access Rights		
			□ View Only □ Full		
			☐ View Only ☐ Full		
			☐ View Only ☐ Full		
			□ View Only □ Full		
			□ View Only □ Full		
			□ View Only □ Full		
			☐ View Only ☐ Full		
			□ View Only □ Full		
Requested Action:	Idau				
Access to the Existing Shared Folder Head of Office (owner of the Shared approval from IMS.	shall be approved/authorized by the	e Requested/Authoriz	ed by:		
□ Creation of New Shared Folder Purpose: □ File repository/backup					
□ For information/monit	oring				
□ Collaboration/report o	onsolidation	1	Head of Office		
☐ Others (specify):		(Signature ov	er Printed Name)		
Soft and an active Sales Charles (1980)	AGREEMENT				
I have read and understood the Policies a and hereby agree to abide to these; the DPWH ICT resources and/or be subjected	it any violation thereof shall lead to	Information and Communications the revocation of all my rights	Technology (ICT) Resources and priveleges to access the		
Name of Employee	Signature	Name of Employee	Signature		
	+				
Attested by: (Supervisor's Sign	nature over Printed Name)				
	ION OF REQUEST: Access to				
Approved/Authorized by:	Date Rece		d by:		
Head of Office	Date Com	•	IT Service Desk Analyst		
(Signature over Printed Name)		(Sig	nature over Printed Name)		
Action: Approved Disapproved	ATION OF REQUEST: Creation Date Received:		SHARLING STREET		
Action: Li Approved Li Disapproved	Date Received:	Date Completed			
Evaluated by:	Recommending Approv	al: Approve	ed:		
Chief, Systems Administration Section	Chief, Technology Support	- Division	nformation Management Service		
(Signature over Printed Name)	(Signature over Printed		ntormation Management Service nature over Printed Name)		



Bonifacio Drive, Port Area, Manila

PERSONALLY-OWNED DEVICE (POD) CONFIGURATION REQUEST FORM

				Service Request No.:
			REQUEST	
Date of Applica	tion:			Employment Status:
Employee Name	e:			□ Regular Employee
Office:		(Last Name, First Name		□ Casual / Job Order / Trainee
		(Office, Division,		(Contract expires on)
Position:				□ Consultant / Contractor / Supplier (Contract expires on)
Contact Numbe	r (Local):			_
Device Type:	☐ desktop com	puter 🛘 🗆 laptop compute	er 🛘 mobile tablet 🗘 mo	obile phone
Brand and Mode	el:		Additional information	on, if any:
Reason:				
□ No availabl □ Others	le DPWH-issued	device	☐ The DPWH-issued the system being	device is incompatible with accessed
Access requirem	nents: 🗆 None			
☐ Internet co	nnection	☐ Email system	☐ Application system (specify)
☐ Network pr	rinter	☐ Shared file storage	☐ Intranet website	□ Others
	TOWN HELD		AGREEMENT	
I acknowledge a			ions related to the use of my	device for work purposes under the Department's
I will take reaso	nable steps to se	ecure my device, such as u	sing a strong password and ir Department's data stored on	nstalling an updated security software. I understand
				from unauthorized access. I acknowledge that I am
responsible for t	the backup and r	ecovery of data on my dev	ice.	
I agree and give understand that	e full consent for this may involve	IMS/IT Support Officer to removal of software that i	configure my device in accord is not consistent with the Dep	dance with the standards of the Department. I partment's policies or may pose security risks.
		harmless for any damage o heft of my device or any da		y device for work purposes. This includes any
and hereby agre	e to abide to the		eof shall lead to the revocatio	n and Communications Technology (ICT) Resources on of all my rights and priveleges to access the
				
		(Employe	e's Signature over Printed Name)
Attest	ted by:		F	Requested/Authorized by:
	Superv	risor	-	Head of Office
	(Signature over F	Printed Name)	On the American Inc.	(Signature over Printed Name)
		EVALUATION	OF REQUEST (to be filled or	ut by IMS)
Date Received:			Date Completed:	
Action:			Remarks:	
☐ Approved	☐ Disapprove	d		12.5
Evaluated by:		Recomm	mending Approval:	Approved:
100 LSA V. 200 - 2 V. 25 - 2 V	Administration Sect	101010	Technology Support Division Inature over Printed Name	Director, Information Management Service (Signature over Printed Name)



SOFTWARE REQUEST FORM

Bonifacio Drive, Port Area, Manila

			Servi	ce Request No.: _		
		REQUEST				
Date of Applicat	tion:					
Office:						
Contact Numbe	r (Local):	(Office, Division, Section)				
Server Access ☐ Software inst ☐ License use ☐ Others (speci	allation	Specifications:				
Requested Ac	tion: (Please check where	applicable)				
Name of	Employee	Software	Version	To b	e installed	on
				□ Desktop	☐ Laptop	□ Server
				☐ Desktop	□ Laptop	☐ Server
				☐ Desktop	☐ Laptop	☐ Server
				☐ Desktop	□ Laptop	□ Server
				☐ Desktop	□ Laptop	□ Server
				□ Desktop	☐ Laptop	□ Server
Purpose:	1					
	Head of Office (Signature over Printed Nar	ne) AGREEMENT				
and hereby agre		and Guidelines on the Use of DPWH any violation thereof shall lead to the plinary actions.				
Nam	e of Employee	Signature	Name of Emplo	oyee	Signa	ture
Attest	ted by:					
	Supervisor's Signature over Pri	nted Name)				
New York Committee	to the letter to the time of	EVALUATION OF REQUEST (to	he filled out by IMS)			
Date Received:						
			mpleted:			
Action: Approved	☐ Disapproved	Remark	(S:			
Evaluated by:		Recommending Approva	l:	Approved:		
Chief, Systems	Administration Section over Printed Name)	Chief, Technology Support (Signature over Printed N			mation Manage	



Bonifacio Drive, Port Area, Manila

TELEPHONE LINE AND/OR FEATURE ACTIVATION REQUEST FORM

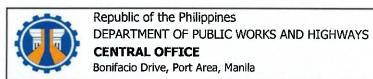
				Service Request No.:		
	1200	RI	QUEST			
Date of Application:				Employment Status:		
Employee Name:	☐ Regular Employee					
Office:	Court / Joh Ouder / Turings					
Office.						
Position:				☐ Consultant / Contractor / Supplier		
Contact Number (Local):				(Contract expires on)		
Average number of telephone calls:						
Nature	Daily	Weekly	Monthly			
International						
National (other than DPWH offices) National (DPWH offices)						
Requested Action: (Please check where a	pplicable)					
Type of Access				Purpose / Reason		
☐ Telephone Line	+					
Telephone Outlet	+					
☐ International Direct Dialing (IDD) ☐ National Direct Dialing (NDD)	+					
National Direct Dialing (NDD)						
Requested/Authorized by:						
U						
Head of Office (Signature over Printed Name	·)					
		AGR	EEMENT			
I have read and understood the Policies and	d Guidelines	on the Use	of DPWH Infor	mation and Communications Technology (ICT) Resources		
and hereby agree to abide to these; that any	violation t	hereof shall	lead to the revo	cation of all my rights and priveleges to access the DPWH		
ICT resources and/or be subjected to discipli	inary actions	5.				
Attested by:						
(Employee's Signature over Printed	Name)			(Supervisor's Signature over Printed Name)		
E	VALUATI	ON OF RE	QUEST (to be f	illed out by IMS)		
Date Received:			Date Comple	eted:		
Purpose: (Please check where applicable)						
☐ research, procurement, public information, edu		aining		g/uploading of data from/to external offices/agencies		
infrastructure planning, design and construction	า			tion and/or submission of reports with internal/external offices		
☐ calamity and disaster operations ☐ user of the Department's application systems				technical documents and gathering of best practices ent external entities		
☐ Others			rrom amere	ent external entities		
-			Remarks:			
Action: □ Approved □ Disapproved						
Evaluated by:	Rec	ommending	Approval:	Approved:		
Chief, Network Administration Section (Signature over Printed Name)	C		ogy Support Divisi			



Republic of the Philippines DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS CENTRAL OFFICE Bonifacio Drive, Port Area, Manila

VPN ACCESS REQUEST FORM

		Service Request No.:
	REQUEST	
Date of Application:	Employment Status:	
Employee Name:(Last N	Name, First Name, Middle Name)	☐ Regular Employee
Office:	(Office, Division, Section)	☐ Casual / Job Order / Trainee (Contract expires on)
Position:		☐ Consultant / Contractor / Supplier
		(Contract expires on)
Purpose/R	eason	Requirements
☐ WAN connectivity is not available in the of		The User has an existing DPWH-issued
☐ Requires remote access to office files and/	device to be used for VPN access? ☐ Yes ☐ No	
☐ Consistently doing field work		What will be accessed thru VPN?
☐ On vacation leave / study leave / maternit	v leave until	☐ Office computer and files ☐ Intranet website and issuances
	(specify end date)	☐ Network file storage
☐ Others (specify)	·	☐ Application system (specify):
Requested/Authorized by:		
,		
Head of Office		
(Signature over Printed Name)		
	AGREEMENT	
I have read and understood the Policies and Gu and hereby agree to abide to these; that any DPWH ICT resources and/or be subjected to dis	violation thereof shall lead to the revocation	
	Attested i	by:
(Employee's Signature over Printed Nam	ne) (Super	visor's Signature over Printed Name)
EVA	LUATION OF REQUEST (to be filled out by	IMS)
Date Received:	Date Completed:	
Purpose: (Please check where applicable) ☐ research, procurement, public information, education ☐ infrastructure planning, design and construction ☐ calamity and disaster operations ☐ user of the Department's application systems	☐ communication and/or s☐ updating of technical do from different external of	of data from/to external offices/agencies submission of reports with internal/external offices ocuments and gathering of best practices entities
Others		Remarks:
Action: ☐ Approved: ☐ VPN client (GlobalProtect) ☐ ☐ Disapproved	clientless VPN (web portal)	ess
Evaluated by:	Recommending Approval:	Approved:
Chief, Network Administration Section (Signature over Printed Name)	Chief, Technology Support Division (Signature over Printed Name)	Director, Information Management Service



INTRANET ACCESS REQUEST FORM

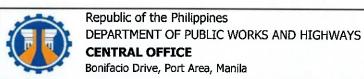
	Service Request No.:			
REQUEST				
Date of Application:	Employment Status:			
Employee Name:	☐ Regular Employee			
(Last Name, First Name, Middle Name) Office:	□ Casual / Job Order / Trainee			
Office: (Office, Division, Section)	(Contract expires on)			
Position:				
Contact Number (Local):	(Contract expires on)			
Note:				
Upon approval of the request, the employee shall have access to the DPWH I (websites with .gov.ph domain). For other ICT services, a separate request for	ntranet Website and other Government Websites orm shall be submitted.			
AGREEMENT				
ICT resources and/or be subjected to disciplinary actions. (Employee's Signature over Print)	ited Name)			
Attested by:	Requested/Authorized by:			
Supervisor	Head of Office			
(Signature over Printed Name)	(Signature over Printed Name)			
GRANTING OF ACCESS (to be filled out by IMS Regional/District IT Support Officer)				
Date Received:	Date Completed:			
DDMM Notwork TD	Yunala mankad kun			
DPWH Network ID:	Implemented by:			
	IT Service Desk Analyst Regional/Distrct ITSO			
	(Signature over Printed Name)			

Please contact the ITSD for more details about this form



INTERNET AND EMAIL ACCESS REQUEST FORM Bonifacio Drive, Port Area, Manila

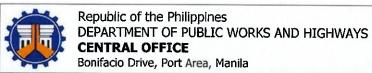
	Service Request No.:		
RE	QUEST		
Date of Application:	Employment Status:		
Employee Name:	☐ Regular Employee		
(Last Name, First Name, Middle Name Office:	□ Casual / Job Order / Trainee		
(Office, Division, Section)	(Contract expires on)		
Position:	☐ Consultant / Contractor / Supplier (Contract expires on)		
Contact Number (Local):			
Requested Action: (Please check where applicable)			
	of Access		
☐ Access private organizations' websites and online platforms	☐ Send email to DPWH Offices		
Purpose/Reason:	☐ Send email to other government agencies and private org.		
	Purpose/Reason:		
The state of the s			
	Email configuration:		
	☐ Increase maximum number of email recipients		
	Purpose/Reason:		
Requested/Authorized by:	☐ Increase mailbox capacity Purpose/Reason:		
	· orpose/reason.		
Head of Office			
(Signature over Printed Name)			
AGRI	EEMENT		
I have read and understood the Policies and Guidelines on the Use	of DPWH Information and Communications Technology (ICT) Resources		
and hereby agree to abide to these; that any violation thereof shall le ICT resources and/or be subjected to disciplinary actions.	ead to the revocation of all my rights and priveleges to access the DPWH		
Ter resources and/or be subjected to disciplinary actions.	Attested by:		
	Attested by.		
(Employee's Signature over Printed Name)	(Supervisor's Signature over Printed Name)		
EVALUATION OF REC	QUEST (to be filled out by IMS)		
Date Received:	Date Completed:		
Purpose: (Please check where applicable)			
☐ research, procurement, public information, education and training	☐ downloading/uploading of data from/to external offices/agencies		
☐ infrastructure planning, design and construction ☐ calamity and disaster operations	☐ communication and/or submission of reports with internal/external offices ☐ updating of technical documents and gathering of best practices		
☐ user of the Department's application systems	from different external entities		
□ Others	Remarks:		
Action:			
☐ Approved: ☐ internet access ☐ external email ☐ internal email ☐ increase maximum number of reci			
□ Disapproved			
Evaluated by: Recommending	Approval: Approved:		
Chief, Systems Administration Section Chief, Technolog	gy Support Division Director, Information Management Service		
700 PM v 1	gy Support Division Director, Information Management Service er Printed Name) (Signature over Printed Name)		



CHANGE OF NETWORK ACCOUNT REQUEST FORM

	Service Request No.:				
REQUEST					
Date of Application:					
Registered Employee Name:	Application user: ☐ Yes ☐ No				
A not blong First blong Middle Street					
Office: (Office, Division, Section)	List of applications being used:				
Contact Number (Local):					
Requested Action:					
Change of Name and Network ID due to:	s of the Philippines				
	of the Philippines				
Updated Employee Name: (Last Name, First Name, Middle Name)	-				
AGREEMENT					
I hereby certify that the information provided in this document is true, accurate and in accordance with the relevant governing laws of the Philippines.					
(Employee's Signature over Printed Name)					
Attested by:	Requested/Authorized by:				
Supervisor (Signature over Printed Name)	Head of Office (Signature over Printed Name)				
GRANTING OF CHANGES (to be filled out by IMS)					
Date Received:	Date Completed:				
Updated Network ID:	Implemented by:				
Updated email address:					
	IT Service Desk Analyst (Signature over Printed Name)				
	/- ^				

Please contact the ITSD for more details about this form



COST ESTIMATION APPLICATION (CEA) ACCESS REQUEST FORM

				Servi	ce Re	quest No.			Wo	rk Order	No		
				RE	QUE	ST	No.	115153	19.18				
Date of Application:													
Office/Division/Section:									_				
Employee Name	Par Sale	Shell			Tale.	May Est	STATE OF THE PARTY	HERE	Us	er Gro	dn	TO BELLEVIOR	Sec.
(Last Name, First Name Middle Initial)	Employ	ee ID		Netv	vork	ID	AA	CEM	CETL	CETM	CERM	CERTL	CERTM
			Г										
													6 6
			-										
			_										
EGEND (for User Group)	***************************************												
AA Application Administrator CEM Cost Estimation Manager CETL Cost Estimation Team Lea CETM Cost Estimation Team Me	der					CERMCERTCERT	L Co	ost Estima ost Estima ost Estima	tion Rev	iew Tea	m Leadei		
	No.	Tely)		AGRE	EM	ENT		BALL	PARTIE	THE R		1805	ALL
have read and understood the Policies nd hereby agree to abide to these; tha Tresources and/or be subjected to d	t any violat	tion the	reof	e Use o f shall le	f DP ead to	WH Inform the revo	nation a cation	and Comi of all my	municati rights a	ions Tec nd privil	hnology eges to a	(ICT) Reaccess th	esource ne DPW
Employee Name	TO BELLS	Signati	ure	3000									
					Att	ested by	:						
													
			_	-			Super	visor's Sig	nature	over Pri	nted Na	me	
							SHOW						
				UTHO			13.			1011		5000	1930
		К	equ	uest Al	JENO	rized by:							
				Hand.		· · ·							
		(Sig	ınat	Head over	_	rice nted Name	e)						
	EVALUA					(to be fille		NV BOC)	-		14.321	S POPER	1970
ate Received by Bureau of Constr	THE RESERVE TO THE					(to be inte	out i	, 500				all are	
Employee Name		pleted	Tra	inina		Δ.	pprov	al			Rema	wko.	
		Yes		No		Approved	pp.01	Disappr	oved		Kema	II KS	D. BULLE
	一百	Yes		No		Approved		Disappro					
		Yes		No		Approved		Disappr					
		Yes		No		Approved		Disappro					Ī.
		Yes		No		Approved		Disappro	oved				
					Apj	proved by	/ :						
								Application				7	
	GRAN	ITING	OF	ACCES	SS (1	o be filled			9,576	- ME		1980	400
ite CEA User Access has been gra													
					-								
	1	mplem	ent	ed by:									
								Applicati	on Sun	ort Por			
							(9	Signature					



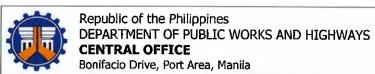
CUSTOMER SATISFACTION SURVEY APPLICATION (CUSSA) ACCESS

		Servi	ce Request No			Work C	rder No		
		REC	QUEST	e week to	A CONTRACTOR		GERN	BRR	BUS
Date of Application:									
Office/Division/Section:									
	(T-10 T-10		No. of the last of			11	C		AND DE
Employee Name (Last Name, First Name Middle Initial)	Regional Public Information Officer District Public Information Officer District Public Information Officer AGREEMENT as and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resource at any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH								
				AA	SRS	FDO	CPIO	RPIO	DPIO
EGEND (for User Group) AA Application Administrator SRS Stakeholders Relations Some FDO Front Desk Officer			• RI	PIO Re	gional Public	Inform	ation Offic	er	
		AGRE	EMENT						
T resources and/or be subjected to d Employee Name	lisciplinary actions		au to the rev	OCALIOI O	e all my righ	us and p	privileges	to access	tne DPW
			Attested	by:					
				Superv	/isor's Signa	ture ov	er Printed	Name	
		AUTHOR	ZIZATION	DESIGNATION OF THE PERSON OF T			The same		1500
	R	equest Au	thorized b	y:					
	THE RESERVE	nature ove	of Office r Printed Na	_	3.510000				
THE RESIDENCE OF THE PARTY OF T	EVALUATION	OF REQU	EST (to be	filled out b	y SRS)			A FINE	MARKE
ate Received by Stakeholders Rel	ations Service:								
Employee Name	Completed	Training		Approva			Re	marks	Ber
	Yes	No	Approv		Disapproved	_			
	Yes	No No	Approve		Disapproved				
	Yes	No No	Approve		Disapproved	_			
	Yes	No	Approve		Disapproved Disapproved	1			
			-		Disapproved	Ч.			
			Approved	_	8 li ti 1				
					Application (Signature ov				
CALAS PROPERTY AND A PROPERTY AND	GRANTING	OF ACCES	SS (to be fille	MARKET STREET		14-120		0.12	
nte CuSSA User Access has been g						THE REAL PROPERTY.			
		mented by	 :						
					Application Signature ov)	

Republic of the Philippines DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS CENTRAL OFFICE Bonifacio Drive, Port Area, Manila

CIVIL WORKS APPLICATION (CWA) ACCESS

		Serv	rice Request No)	W	ork Order	No	
		RE	QUEST	HE THIS AND			ONE DATE	BUSY ST
Pate of Application:								
ffice/Division/Section:								
Employee Name		E SOUTH	A FOREST		TO SERVICE	Jser Grou	in and	6-8-8
(Last Name, First Name Middle Initial)	Employee ID	Net	work ID	SUP	RUIC	vw	UPMO	RO/DEC
				501	,,oac		Orno	KO/DEC
778 7 8 7 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8								
GEND (for User Group)								
- SUP Supervisor			• UPM		O Coordinato			
 RUIC Registry Updating & Issue VW View for Administrative P 			• RO/	DEO Regi	onal/District	Eligibility		
LIVE BOOK STATE OF THE STATE OF								
		AGR	EEMENT			539	PERM	
eve read and understood the Policies	s and Guidelines or	the Use	of DPWH Info	rmation an	d Communica	ations Tec	hnology (IC	T) Resou
I hereby agree to abide to these; that resources and/or be subjected to d	at any violation the	reof shall	lead to the re	vocation of	all my rights	and privile	eges to acce	ss the Di
			1					
Employee Name	Signatu	ire						
			Attested	by:				
				Supervis	or's Signatur	e over Pri	nted Name	
		AUTHO	RIZATION	THE ROLL	A STATE OF THE PARTY OF THE PAR	E GE	THE REAL PROPERTY.	23 64
	R	equest A	uthorized b	y:				
		•						
<u> </u>		Head	of Office					
	(Sig		er Printed Na	me)				
	EVALUATION	OF REQ	UEST (to be	filled out by	PrS)		DATE:	HEER
e Received by Procurement Ser	vice:							
Employee Name	Completed '	Training	1 5 6 6 6	Approval	BROWN	STEP LET	Remarks	THE REAL PROPERTY.
	Yes	☐ No	Approv	ed	Disapproved			
	Yes	☐ No	Approv	ed 🔲	Disapproved			
	Yes	No	Approv		Disapproved			
	Yes	No	Approv		Disapproved			
	Yes	No	Approv	ed	Disapproved			
ommended by:			Approved	hv:				
······································			7.pp.0104	~,·				
Application User Co	ordinator				Head of	Office		
(Signature over Print				(Si	gnature over		ame)	
	GRANTING	OF ACCE	SS (to be fille	ed out by IM	IS)			THE REAL PROPERTY.
e CWA User Access has been gra	anted:							
	Implem	ented by	:					
				Δ:	pplication Su	pport Pers	son	
				(Sig	nature over	Printed Na	ame)	



DESIGN MANAGEMENT APPLICATION (DMA) ACCESS REQUEST FORM

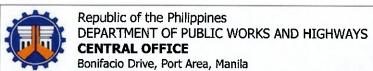
				Servi	ce Reque	est No			Wor	rk Order	No		
	1371	HE VIG		RE	QUEST	The state of	a land	Manual Property of the Parket	SPECIE	WATE:	3800	(EMB)	
Date of Application:					Manager Control								
Office/Division/Section:													
HER PROPERTY VEHICLES					TO SECOND				Us	er Grou	ın		Dr. Co.
Employee Name (Last Name, First Name Middle Initial)	Emplo	yee ID		Netv	vork II		11-0	Design	Team			view Te	am
(Last Raine, First Haine Middle Millar)			1	ME			DM	DTL	DSTL	DTM	RDTL.	RDSTL	RDTM
													E
			_										
			_										
			-			-							
EGEND (for User Group)													
DM Design Manager					•	RDTL			sign Tean				
 DTL Design Team Leader DSTL Design Sub Team Leader 					:	RDST.		eview De eview De	sign Subʻ sign Tean	Team Le n Membe	ader er		
DTM Design Team Member													
	4.369			AGRE	EMEN	Tilli			TEN	139-30	Parl In	The state of	THE REAL PROPERTY.
have read and understood the Policies	and Guid	delines o	n th	e Use o	of DPWH	Inform	ation	and Com	municati	ons Tec	hnology	(ICT) D	ocource
nd hereby agree to abide to these; tha	at any viol	ation the	reof	shall le	ead to th	ie revo	ation	of all my	rights ar	nd privile	eges to a	access th	ne DPW
T resources and/or be subjected to d	isciplinary	actions							_				
Employee Name	A PART	Signati	ure	MAGN									
					Attes	ted by:	:						
							Super	visor's S	ignature	over Pri	nted Na	me	
	100100		AI	ITHOR	RIZATI	ON	7700	NAME OF TAXABLE		SER	F-341/18	A Data	
			1000	STATE OF THE PARTY OF	uthoriz				A STATE OF THE PARTY OF THE PAR				
			·cq:	Jest A	utiloi iz	eu by.							
				11	-6.060				<u>. </u>				
		(Sid	onat		of Office er Printe		رد						
	EVALS	LOUIS DE		-		_	_	I. DODY	SELVE	III Service			5-5-6
		IATION	Ur	REQU	JE31 (t	o be fille	ed out	DA ROD)			The state of		
ate Received by Bureau of Desigr	l:												
Employee Name	Com	pleted	Tra	ining		A	pprov	al		No.	Rema	irks	SAN S
		Yes] No	A	pproved		Disapp	roved				
		Yes		No	A	pproved		Disapp	roved				
		Yes		No	A	pproved		Disapp	roved				
] Yes] No	☐ A	pproved		Disapp	roved				
		Yes		No	☐ A	pproved		Disapp	roved				
					Appro	val:							
								Applicat	ion Haar	Coordin			
									ion User e over Pi				
	CDA	NTING	0E	ACCE	SC /to	no filled		THE PERSON NAMED IN	75 (29)			15 35 79	N 1022
		HITING	Vľ	ACCE	33 (10 1	Denni S	out by	TIME	2000	A PARTY	13.44		
ate DMA User Access has been gra	anted:												
		Implem	ient	ted by:	:								
								Applica	tion Supp	ort Per	son		_
							(e over Pr				



Republic of the Philippines DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS CENTRAL OFFICE Bonifacio Drive, Port Area, Manila

DOCUMENT TRACKING SYSTEM (DoTS) ACCESS REQUEST FORM

	William Property							16000
Service Request No								
fice/Division/Section:								
Employee Name				User	Group	1230	Module	111
(Last Name, First Name Middle Initial)	Employee 1	D	Network ID	PU	DC EU	GD	CS	CV
GEND (for Licer Croup)								
			- 60					
EU End User			- CW					
					AND REAL PROPERTY.	The state of	Victoria de la constante de la	
					STATE OF			58
ave read and understood the Policies	and Guidelines or	n the Use o	of DPWH Informat	tion and Comn	nunications T	echnolog	gy (ICT) F	Resou
resources and/or be subjected to di	any violation the sciplinary actions.	reor snali i	ead to the revoca	tion of all my r	ignts and priv	/ileges to	o access t	ne Di
	o.g.i.a.t.							
			Attested by:					
			S	upervisor's Sig	nature over i	Printed N	lame	
		AUTHO	RIZATION	REBAIL	Charles and the same of the sa	HAR	BEAS.	
	R	equest A	uthorized by:					
		Head	of Office		_			
	(Sig	nature ov	er Printed Name)					
	EVALUATION	OF REQU	IEST (to be filled	out by HRAS)				
te Received by Records Managen	nent Division: _							
Employee Name	Completed '	Training	App	proval	CR UNS	Ren	narks	N/A
	Yes	No	Approved	Disappro	oved			
	Yes	☐ No	Approved	Disappro				
	Yes	☐ No	Approved	Disappro	oved			
	Yes	No	Approved	Disappro	oved			
	Yes	☐ No	Approved	Disappro	ved			
			Approved by:					
				Applicatio	n User Coord	finator		
					over Printed			
	GRANTING	OF ACCE	SS (to be filled ou	ut by IMS)				
te DoTS User Access has been gra	inted:							
	Implem	ented by	:					
				4 1 1	on Support P			



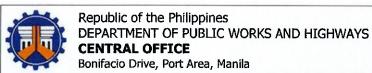
ELECTRONIC BUDGET SYSTEM (eBudget) ACCESS

				Servi	ce Re	equest No			Work O	rder No		
		State Line	118	REC	QUE	ST	Min	ENERGY.	NO.	A SAME	MANAGE	
Date of Application:												
Office/Division/Section:												
Employee Name							Harris .	300	User	Group	7855A	
(Last Name, First Name Middle Initial)	Emplo	yee ID		Netv	vorl	(ID	PR	AP	AU	IT	SA	AUC
			-								3/2	
			\vdash									
			\vdash				-					
EGEND (for User Group)												
PR Preparation AP Approval						IT SA		Support Offic stem Adminis				
AU Auidt / Read Only						- AUC		ta Steward /				
				AGRE	EM	ENT		Mark Hall				1132
have read and understood the Policies	and Gui	delines o	n th	e Use o	f DP	WH Inform	ation a	nd Commun	ications	Technol	ogy (ICT)	Resourc
nd hereby agree to abide to these; tha CT resources and/or be subjected to d	t any vio isciplinar	iation the y actions	reo	r snall le	ead t	the revoc	ation o	if all my right	ts and p	orivileges	to access	the DPV
Employee Name		Signati	ure									
					Δ	ttested by	, <u>.</u>					
					-	,	-					
	+				-		Super	/isor's Signal	ture ov	er Printed	1 Name	
	Carlo M		Δ	UTHOR	777			5000000	D. II	CO VAN		
						rized by:	MORE					
			4	acot At		rized by:						
<u> </u>				Head (of O	ffice						
		(Sig	gnai	ture ove	r Pr	inted Name)					
	EVAL	NOITAU.	N O	FREQ	JES	T (to be fill	ed out	by FS)			TAIL.	
ate Received by Finance Service:			_									
Employee Name	Cor	npleted	Tra	ining		A	prova			Re	emarks	918810
	 	Yes	H	No	F	Approved	-	Disapproved	_			
	++	Yes	누	No No	늗	Approved	-	Disapproved	_			
		Yes	一	No	十	Approved Approved	\vdash	Disapproved Disapproved				
		Yes		No		Approved		Disapproved	_			
ecommended by:					A	pproved b	y:	and the same				
Application User Co				—	-				of Offi			
(Signature over Prin	77.77.77		1000		152.00	TO THE PARTY OF	1700	Signature ov	er Print	ted Name	;)	
CANCEL CONTRACTOR			OF	ACCES	SS (to be filled o	out by I	MS)			2013	NEW YORK
ate eBudget User Access has beer	grante	d:										
		Imple	mei	nted by	' :							
					_			Application :				



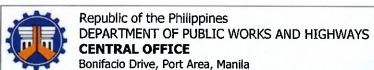
ELECTRONIC NEW GOVERNMENT ACCOUNTING SYSTEM (eNGAS) ACCESS REQUEST FORM

				Service Rec	uest No			Work O	rder No		
		TO BE		REQUES	T		THE PARK	11935	HAR	HIPPO	
ate of Application:											
ffice/Division/Section:											
Employee Name	Emplo	yee ID		Network	TD.		SAN PER	User (Group	SECTION AND ADDRESS OF THE PERSON ADDRESS OF THE PERSON AND ADDRESS OF THE PERSON AND ADDRESS OF	560
(Last Name, First Name Middle Initial)	Limpio	,cc 1D	10/6	TECHOIR	STEP IN	PR	AP	AU	п	SA	AU
					-						
GEND (for User Group)											
PR Preparation					• IT		Support Office				
 AP Approval AU Auidt / Read Only 					• SA • AUC		stem Administ ta Steward / A				
	485			GREEME		CONTRACT OF THE PARTY OF THE PA				515318	
ave read and understood the Policion d hereby agree to abide to these; the these; the same the same are the	es and Guid nat any viol	Jelines or ation the	n the l ereof si	Jse of DPV nall lead to	VH Informa the revoc	ation a ation o	nd Communi f all my right	cations s and n	Technolo rivileges	ogy (ICT)	Resou
resources and/or be subjected to	disciplinary	/ actions					· con triy rigino	o and p	muges	to decess	uic Di
Employee Name	THE DEEP	Signati	ure								
	_			At	tested by	':					
						Super	/isor's Signat	ure ove	r Printed	Name	
	B (B) (B)	THE SALE	AUT	HORIZA	TION	Harris	10 Te 187			A COL	200
		R	Reque:	st Author	ized by:						
_											
		/Ci/		ead of Off		`					
THE RESIDENCE OF THE PARTY OF T	EVAL			e over Prin			FC\	4000	100000	600 (S) April	
te Received by Finance Service		DATION	V OF I	KEQUEST	(to be fille	ed out i	DY F5)				
Employee Name		npleted	Train	ina	Ar	prova	1		Do	marks	
		Yes		0	Approved	Piova	Disapproved		Re	marks	1378
		Yes			Approved		Disapproved				
		Yes		。	Approved		Disapproved				
		Yes			Approved	$ \vdash$	Disapproved				
		Yes		о <u> </u>	Approved		Disapproved				
wanted a second											
commended by:				Ap	proved by	y:					
-	Coordinator			A p	proved by	y:	Head	of Offic			
commended by: Application User C (Signature over Pri				Ap	proved by		Head Gignature ove	of Officer Printe)	
Application User C	inted Name	2)	OF A	App		(5	Signature ove)	
	inted Name GRA	e) NTING	OF A			(5	Signature ove)	
Application User C (Signature over Pri	inted Name GRA	NTING		CCESS (to		(5	Signature ove)	
Application User C (Signature over Pri	inted Name GRA	e) NTING		CCESS (to		(S	Signature ove	er Print	ed Name)	



INFRASTRUCTURE RIGHT-OF-WAY MANAGEMENT APPLICATION (IROWMA) ACCESS REQUEST FORM

			Ser	vice Request No				Order			
	Ta (22) 30	STATE OF		QUEST	W. P. J. S.	13 /3 / 3 / 3 · 3	VVOIR	Order	NO.	EULESIA .	
Pate of Application:		7.57		Q0E31		Np. 9.11				05010	
Pate of Application: Office/Division/Section:											
Trice/ Division/ Section:											
Employee Name		Emp	loyee ID	Network 1	(D			Use	Grou	p	
(Last Name, First Name Middle I	nitial)		,			OF IO	TL	SP	AUC	MANCOM	ADM:
		-				-					
							-				
GEND (for User Group)											
HEAD OF IO Head of Implem TL ROW Team Lead SP ROW Specialist				AUC MANCOM ADMIN	Mana	ation Use gement C MA Admi	ommit	tee	r		
SECTION OF THE PROPERTY OF THE PERSON OF THE		1130	AGR	REEMENT	33500				Refe		
ave read and understood the Polic	ies and Guid	elines n			ation and	l Commi	nicatio	on Tec	chn olog	ny (TCT\ D	00011
d hereby agree to abide to these; ti	hat any viola	tion the	reof shall	lead to the revoca	tion of a	ll my righ	its and	l privil	eges to	access th	ie DP
Γ resources and/or be subjected to											
Employee Name		Signati	ure								
	_										
	_			Attested by:							
				1							
]	Superviso	or's Signa	ture c	over Pi	rinted N	lame	
		WE TH	AUTHO	RIZATION	AUM		3	TOTAL		TE SALE	4
		R	Request A	Authorized by:							
_											
		/Si/		of Office ver Printed Name)							
NATIONAL PROPERTY AND ADDRESS OF THE PARTY AND	PVALL		-			1.00		Will the	1000	100000	N/A
	EVALU	MITOL	Y OF RE	QUEST (to be filled	d out by	LS)					
te Received by Legal Service:											
Employee Name	Com		Training		proval				Rem	arks	
		Yes	No No	Approved		isapprove					
		Yes	No	Approved Approved		isapprove isapprove					
		Yes	No	Approved		isapprove					
		Yes	☐ No	Approved		isapprove	d				
ecommended by:				Approved by:							
bedinnended by				Approved by:							
Application User ((Signature over Pri					(Sia	Head nature ov	of Off		ame)		
(Signature over 11)		UTTNIC	OF ACC	ESS (to be filled as		NAME OF TAXABLE PARTY.	CI FIII.	iccu ive	anie)	or House	112 113
to TDOWMA Upon Across here by		The same of the sa	OF ACC	ESS (to be filled or	at by IMS)	1000				
te IROWMA User Access has be	sen grante										
		Imple	mented l	y:							
					A	plication	Cunn	ort Do	rcor		
						pplication nature o					



MULTI-YEAR PLANNING AND SCHEDULING APPLICATION (MYPS) ACCESS REQUEST FORM

		Sen	vice Req	uest No.				Wor	k Orde	r No			
	THE REAL PROPERTY.	RI	EQUES	т	SHIT	BONE B	1814				1/82	Res	
ate of Application:												0.000	
ffice/Division/Section:													
		Land Contract		LANGE	on the		Hen		-	-			-
Employee Name (Last Name, First Name Middle Initial)	Employee ID	Network ID	DPC	DPD	DPD	FAPs	PD	r Gro	PPC	RPC	Read	UPC	ADM
(Last Maine, First Name Product Linus)	10	ID	DPC	Admin	Coor	Coor	Admin	Coor			Only		
									-				
				-	_								
	-												

GEND (for User Group)													
DPC District Planning	Coordinator			. 00	Coor	Dro	jrammi	an Div	dolan C	·			
 DPD Admin Development Pla 	nning Division A	dministrator		• PP	C	PIP	Plannir	ıg Coo	rdinate	or			
DPD Coor Development Pla FAPs Coor Foreign Assisted				• RP			ional Pl IO Plan				٢		
PD Admin Programming Div					MIN		S Admi			u			
		AGR	EEME	NT							COAL ST	18	MA
ve read and understood the Policie	s and Guideline	es on the Use	of DP\	NH Info	rmatio	on and	Comm	unicat	tion Ta	echnol	logy (Ti	(T) D,	acou
hereby agree to abide to these; the	at any violation	thereof shall	lead to	the rev	ocatio	n of all	my ria	ihts ar	nd priv	ileaes	to acc	ess th	e DF
resources and/or be subjected to o	disciplinary acti	ons.					,						
Employee Name	Sign	nature	1										
			1										
			1										
			Att	tested	by:								
	_		1										
			-		Sur	perviso	r's Siar	ature	over l	Printer	l Name		_
TO THE OWNER OF THE PARTY OF TH]										10.00
	SHIP SHIP	AUTHO		Service Communication of the C									
		Request /	Author	ized by	/:								
								_					
			of Off		,								
		(Signature ov		THE RESERVE TO SERVE									
		ON OF REC	QUEST	(to be	filled o	ut by P	S)						
e Received by Planning Service	:												
Employee Name	Complet	ed Training			Appro	oval				Re	emark	s	
	Yes	No No		Approve	ed [Dis	approv	ed					
	Yes	No No		Approve	d [Dis	approv	ed					
	Yes	No No		Approve	d [\neg	approv						
	Yes	No No		Approve	7		approve						
	Yes	No		Approve		_	approve						
commended by:			Apı	proved									
			,		•								
Application User Co								d of O					_
(Signature over Prin	ted Name)					(Sign	ature o	ver Pr	inted N	lame)			
	GRANTI	NG OF ACC	ESS (to	be fille	d out l	by IMS							
MYPS User Access has been g	ranted:												
	Im	olemented b	y:										
			_		_								
							olicatio:						



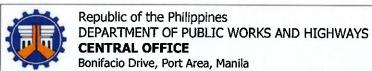
PROJECT AND CONTRACT MANAGEMENT APPLICATION (PCMA) ACCESS

		Serv	ice Request	No		Work	Order No		
		RE	QUEST		334	Robbs	ALLES		
Date of Application:									
Office/Division/Section:						_			
	Employee	- S - S - F - F - S	300000		U	ser Grou	ID .	100000	
Employee Name (Last Name, First Name Middle Initial)	ID	Network ID	RD/ARD	DE/ADE	CCD/CCS	MoE	PM	PE	PI
			1.0//1.00	DEJABE	5557555	FIOL	L. Charte		
LEGEND (for User Group)									
RD/ARD Regional Directo	r / Assistant Re	gional Director				onitoring E			
 DE/ADE District Engineer CCD/CCS Chief, Constructi 	/ Assistant Dis on Division / Se	trict Engineer ection				oject Mana oject Engi			
			-		PI Pi	oject Insp	ector		
	STATE OF		EEMENT			to the	MA SERVICE	1000	ART M
I have read and understood the Polici	es and Guideli	nes on the Use	of DPWH I	nformatio	n and Com	municatio	ns Technol	ogy (ICT)	Resources
and hereby agree to abide to these; the contract of the contra	nat any violatio disciplinary ao	on tnereor snall I ctions.	ead to the	revocatio	n of all my	rights and	i privileges	to access	the DPWH
Employee Name		nature							
			Attest	ed by:					
				Supe	rvisor's Sig	nature ov	er Printed	Name	
		AUTHO	RIZATIO	N				17-2	HE SHE
		Request A	uthorized	l by:					7946
			of Office						
		(Signature ov	The same of the same of						
	EVALUAT	TION OF REQ	UEST (to	be filled ou	ut by BOC)				Philip
Date Received by Bureau of Cons	truction <u>:</u>								
Employee Name	Compl	eted Training		Appro	oval		Re	emarks	HORA
		res No		roved	Disappi				
		res No		roved	Disapp				
		res No		roved [Disappi Disappi				
		res No		roved	Disappi				
			Approved			0,00			
			Approved						
					Applicatio	n I ker Co	ordinator		_
					(Signature				
	GRANT	TING OF ACCE	SS (to be	filled out I	by IMS)			BALL	THE SAME
Date PCMA User Access has been	granted:								
				_					
	Imp	lemented by:							
					Applicati	on Suppor	t Person		_
					(Signature				

Republic of the Philippines DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS CENTRAL OFFICE Bonifacio Drive, Port Area, Manila

PERSONNEL INFORMATION SYSTEM (PIS) ACCESS

Bollilacio Blive	, Forcarea, M	arnıç			40.0									200				
				Servic	e Requ	iest No	· —				_ V	/ork (Order	No				
开放性态的态度		ALC: NO.		REC	UES	T												
Date of Application:																		
Office/Division/Section: _																		
THE RESIDENCE OF THE PARTY OF T	3/07/201	AT THE		11/4/1/18	1916		ı	Jser	Grou	מו	elti		UB			100	530	100
Employee Name (Last Name, First Name Middle	Employee ID	Network ID	k	111119		C	0				R	10	D	EO		Mod	lule	00
(Last Name, First Name Middle Initial)	10	10		CDD EW	B ES	PPS	RM	SU	то	RO	RA	RO	DA	RO	PL	PD	LV	LB
			+															
LEGEND For User Group						For Mo	adule											
CDD Capacity Development	• SU	Super Admir	1			- PI		Plant	illa									
 EWB Employee's Welfare & Be ES Employment Staffing 	nefit = TO * RA	TAS Officer Regional Ad				• PI	D		nnel C	ata								
PPS PPS Payroll & Personnel: RM Records Management		District Adm Read Only				- LE		Libra	•									
	STATE VALUE OF	TO MENT		AGRE	EME	ST.	SON	80.8	1010	1500	Contract Con	280	hedr	e Price	1000	600	7000	CN TO
I have read and understood the	Policies and Co	idolinas on						lilan a				- 4.1		.l l	2000			
and hereby agree to abide to the	ese; that any vi	olation ther	eof	shall le	ad to	the re	voca	tion a	of all	my ri	iunici ights	auon and	s rec privil	eaes	ogy (to ac	cess	keso the D	DPWF
ICT resources and/or be subjec	ted to disciplina	ary actions.																
Employee Name	VAR B	Signatu	re	13.9														
					A	ttest	ed b	v:										
								•										
					_			Supe	erviso	r's Si	anat	ure o	ver i	Printe	d Na	me		
					J. C. C. T.	Sept.	163.0				J			7				
	C. Carrie		AU	THOR	IZAT	ION												
		Re	equ	est Au	thori	zed b	y:											
		02004		Head o														
		(Sig	natu	ire ove	r Print	ed Na	me)											
	EVAL	UATION O	OF F	REQUE	EST (o be f	illed	out b	y HRA	AS)								
Date Received by Human Re	source and A	dministrat	ive	Servi	ce:													
Employee Name	Co	mpleted 7	rai	ning	11/2	M. Ba	App	provi	al		76	316	30	Rei	mark	cs	gi ki	100
	[Yes		No		Approv	ed		Disa	approv	ved							
		Yes		No		Approv	ed] Disa	ppro	ved							
		Yes		No		Approv	ed		Disa	ppro	ved							
	L	Yes	닉	No		Approv			Disa	ppro	ved							
		Yes		No		Approv	ed	L	Disa	ppro	ved							
Recommended by:					A	pprov	red I	y:										
Application	User Coordina	ntor			_					— Н	lead	of O	fice				_	
	over Printed Na								(Sigi					Nam	ie)			
	GR	ANTING (OF /	ACCES	S (to	be fille	ed ou	it by	IMS)	HE	H.	40						
Date PIS User Access has be	en granted:																	
		T		الدخوس														
		Tmble	eme	ented l	уу: 					ls -								
									Ap _i	plicat	ion S	Supp	ort Pe	erson				



PROJECT PROCUREMENT MANAGEMENT PLAN APPLICATION (PPMPA) ACCESS REQUEST FORM

				ce Request No QUEST		HOYAGE	k Order No.	STATE OF THE PARTY.	208
e of Application:	A PROPERTY.			SOLO					1000
ice/Division/Section:									
ec/ bitision/ section:									-
Employee Name (Last Name, First Name Middle Initial	E	mployee IE		Network	(ID		User (Group	
(rest state, that statue mudic Illinal						AU	CPA	RPA	DP.
			-						
			+						
	-								
END (for User Group)				***************************************					
e read and understood the Policie	s and Gui	delines on th	ne Use d	EMENT of DPWH Inform	mation and Co	mmunica	tion Techno	ology (ICT)	Reso
nereby agree to abide by these; if If ICT resources and/or be subject	that any v	violation thei	reof sha	II lead to the	revocation of	all my rig	hts and pri	ivileges to	acces
Employee Name	100	Signature	00000						
			-						
				Attested b	y:				
	-				Supervisor's	Signature	over Printe	ed Name	
	1911	A	IITHOE	RIZATION		- January	The state of the s	Zalana	46 (95
	and the same of the			thorized by:					
		/Signat		of Office r Printed Name	۵)				
	EVAL	The second second second	Vancous Vie			NI DE		1000000	0700
Received by Procurement Ser		DATION OF	REQU	(to be fill	led out by PrS)	SE PL			
Employee Name		npleted Tra	ining	A	pproval	1000	R	emarks	
		Yes	No	Approved		proved			
		Yes	No	Approved		5.00			
		Yes	No	Approved		-			
		Yes	No	Approved					
		Yes	No	Approved	Disapp	roved			
mmended by:				Approval:					
Application User Co						Head of (,1	
(Signature over Prin		Difference of the last	ACCE	C (by be Cil.		ire over P	rinted Nam	ie)	
PPMPA User Access has been			ACCE	S (to be filled	out by IMS)		aman	BY LIVE	
	_ · · · · · · · · · · · · · · · · · · ·								
		Implemer	nted by	: 					
							port Persor		



Republic of the Philippines DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS CENTRAL OFFICE

Bonifacio Drive, Port Area, Manila

ROAD AND BRIDGE INFORMATION APPLICATION (RBIA) ACCESS

	· ·					_		_		_	
	San Day San	Service Reque	est No.				Work	Order	NO.	1785	Constant of
		REQUEST		MAKE		13/6		E.		416	
ate of Application:											
ffice/Division/Section:				_							
				THE PARTY OF THE	1200	No. of Concession, Name of Street, or other Persons, Name of Street, or ot		D	oto C	~~~	ity Grou
Employee Name (Last Name, First Name Middle Initial	Employee ID	Network ID	Use	er Group	(Ma	rk on	ly one)	100			ly one)
(Lost Home, First Name Middle Impai	TO BEST AND A	STATE OF THE STATE	SU	GF ICN	RO	BMS	BMS-A PMS	ARDL	OR DESCRIPTION OF THE PERSONS NAMED IN	ADSD	RO/DEO (Please specif
			-				_				
							-				
							_				
GEND (for User Group)			L	LEGEND	(for I	Data S	ecurity G	roup)		
SU RBIA Super User GL GIS & LRS		gement System gement System Admin		ARDL ARDS		IA Data	and LRS and Data Soi	17505			
ICU Inventory and Condition Update RO Read Only		anagement System		• ADSD			forkgroup)	arces			
		ACDEEMEN						T. CO	135 13	1000	
	Charles Tonical River	AGREEMEN		Train in			OCHE !				
ave read and understood the Polici I hereby agree to abide to these; th	es and Guidelines on	the Use of DPWI	Infor	mation ar	nd Co	mmur	nication ⁻	Techi	nology	y (IC	T) Resour
resources and/or be subjected to	disciplinary actions.	or shall lead to th	ie revo	cation or	au m	y rignt	ıs and pr	iviieg	jes to	acce	ss the DP
Employee Name	Signatur	10									
Employee Name	Signatur										
			Atha	مرجا امرام							
			Atte	sted by:							
				Supe	ervisc	r's Sig	gnature o	over	Printe	d Na	me
		AUTHORIZATI	ON	The state of the s			OH DE			1949	100
	Re	quest Authoriz	ed bv:								
		•									
<u> </u>		Head of Office									
	(Sign	ature over Printe		e)							
	EVALUATION (OF REQUEST	to be fil	led out by	PS)		A KONG	BHE	HEAL	HIVE	Red De C
e Received by Planning Service			- Contraction	out by						and the	-
Employee Name	Completed Tr	The second second		pproval	licano	round			Rema	arks	
	Yes		proved proved			roved					
	Yes		proved		- 1	roved					
	Yes		proved			roved					
	Yes		proved			roved					
			,	Ш,			2				
ecommended by:		А	pprov	ed by:							
				-							
Application User Coo	rdinator					Head	of Office				
(Signature over Printed				(S	ignat		er Printe		ame)		
A STATE OF THE PARTY OF THE PAR	GRANTING O	F ACCESS (to b	e filled	out by IM	S)	MAR	10 30			89	23100
ate RBIA User Access has been	AND DESCRIPTION OF RESIDENCE						THE PARTY OF			-	Andrew Street
APEA GOO! ACCOS HOS DECIL	g. arredt										
		Implement	ed hv								
		in plement	ou by:								
							ion Supp				
					1510	nature	e over Pr	inted	ı Nam	ie)	



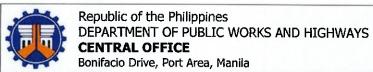
Department of Public Works and Highways IT SERVICE DESK

Information Management Service ICC Building, Bonifacio Drive, Port Area, Manila

REGULAR PAYROLL SYSTEM (RPS) ACCESS REQUEST FORM

3,	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Ser	vice Request No.	W	ork Order No.		_
STATES OF THE STATE OF THE STAT	STATE OF THE PARTY OF	REQU	PROPERTY AND PERSONS NAMED IN	WINDS OF SIA	ork order No.	ELECTIVE	R
Date of Application:	SHEED SHIPPERS	112				MOVE TO SERVICE	
office/Division/Section:							
Thee, Division, Section.	STATE OF THE STATE OF				STATE OF THE PARTY	100 100 100 100	No.
Employee Name	Employee ID	Network ID	Office / Divis	ion / Section	User	r Group	
(Last Name, First Name Middle Initial)				ion y occion	PP FS	PA	P
ET THE STATE OF TH							
							_
GEND (For User Group)	***						
PP Payroll Processor		PA Pay	roll Administrator/Te	eam Lead			
FS Finance Service/Finance	Office User	• P Progr	rammer				
March Control of the		AGREE	MENT	CONTRACTOR OF THE PARTY OF THE	STATE OF THE PARTY OF	700 300 30	101
and and and and the B	-11-1						100
nave read and understood the Pereby agree to abide by these; t	blicles and Guideline hat any violation the	es on the Use of Decreof shall lead to	PWH Information a	and Communication	ı Technology ()	ICT) resour	ces
sources and/or be subjected to d	isciplinary actions.	or or origin read to	and revocation of a	in my ngnos and pr	ivileges to acc	ess the DP	VVIT
Employee Name	Signa	ature					
		Atte	sted by:				
			Superv	risor's Signature ov	er Printed Nam	e	
ENDATORIS ENDER SUCCESSO DUTT A LINE FOR	A PROPERTY IS NOT THE OWNER.	AUTHORI	ZATYON		TANKS OF THE PARTY		
	Hart Control of the C	AUTHORI Request Aut				THE REAL PROPERTY.	
		request rue	nonzed by.				
			055				
		Head of (Signature over					
	EVALUAT		ST (to be filled out b	v HRAS)	Property of the last	THE PERSON NAMED IN	Utr
te Received by Human Resou							
Employee Name		pleted Training		oroval	Re	emarks	
	Yes Yes		Approved Approved	Disapproved Disapproved			
	Yes		Approved	Disapproved			_
	Yes		Approved	Disapproved			
	☐ Yes	☐ No	Approved	Disapproved			
		App	roval:				
				lication User Coord			
STATE OF THE PARTY OF THE PARTY.	CDANT	TNG OF ACCES		nature over Printed	Name)		
ALEGER CONTRACTOR		ING OF ACCESS	(to be filled out by	IMS)	THE STATE OF		
te RPS User Access has been	granted:						
	7						
	ımple	mented by:					
			And	olication Support D	ercon		
				olication Support Pe ature over Printed			

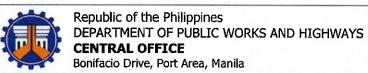
Please contact the IT Service Desk for more details about this form.



ROAD TRAFFIC INFORMATION APPLICATION (RTIA) ACCESS REQUEST FORM

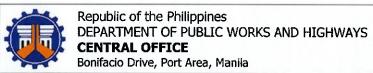
			Service	Request No	w	Work Order No.							
			REQU	JEST	THE REAL PROPERTY.	AND REAL PROPERTY.	THE SE	passage.					
Date of Application:													
Office/Division/Section:													
	7.50					Hear	Group						
Employee Name (Last Name, First Name Middle In	nitial)	E	mployee ID	Network ID	NRTSP COC	NRTSP RC	RO (Please	ADMIN					
		100			Turner coc	THE TOTAL THE	specify)	THE REAL PROPERTY.					
					_								

LEGEND (for User Group)													
 NRTSP COC NRTSP Central Of NRTSP RC NRTSP Regional C 													
ADMIN RTIA Administrate													
			AGREE	MENT		OKOLA.	MATERIA S						
have read and understood the Policies	s and Guid	elines or	n the Use of	DPWH Information a	nd Communic	ation Techr	nology (ICT)	Resource					
and hereby agree to abide to these; tha	at any violai	tion ther	reof shall lead	d to the revocation of	all my rights a	and privileg	es to access	the DPW					
CT resources and/or be subjected to d	isciplinary	actions.											
Employee Name	in the same of	Signatu	ire										
				Attested by:									
				Acceded by.									
					(6:)								
				Supervi	sor's Signatur	e over Print	ed Name						
			AUTHORI	ZATION		Burney.		Service .					
		R	equest Aut	horized by:									
_			Head of	Office									
		(Sig		Printed Name)									
	EVALUA	ATION	OF REQUE	ST (to be filled out by	BOS)		77 19 7,8						
Date Received by Bureau of Quality		THE RESIDENCE OF											
Employee Name			Familia I										
Employee Name	Com		Training	Approval			Remarks	NAME OF BRIDE					
	 	Yes	No [Disapproved								
	+	Yes	No L	Approved	Disapproved								
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	$+$ \vdash	Yes	No L		Disapproved	<u> </u>							
	$+$ \dashv	Yes	No No	7 7	Disapproved								
Recommended by:		ies [Approved by:	Disapproved								
recommended by.				Approved by.									
Application User Co				-	Head of	Office							
(Signature over Print	ed Name)			(Si	gnature over F		e)						
CHARLES TO SERVICE THE SERVICE OF TH	GRAN	ITING (OF ACCESS	(to be filled out by IN	1S)		ALLERS						
ate RTIA User Access has been gr	anted:												
	_												
	;	Implen	nented by:										
					Inglication C	anart Daur							
					Application Su gnature over								



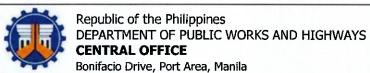
TIME AND ATTENDANCE SYSTEM (TAS) ACCESS

		Service	Request No.		Work Order No			
		REQ	UEST		THE REAL PROPERTY.	THE PARTY		
Date of Application:								
Office/Division/Section:								
Employee Name	CONTRACTOR OF THE PARTY OF THE	I I I I	Ser Printer		User Group			
Employee Name (Last Name, First Name Middle Initial)	Employee ID	Netw	ork ID	ADMIN	РТО	ATO		
				ADMIN	FIO	AIO		
LEGEND (for User Group)					***************************************			
- ADMIN Administrator								
 PTO Primary TAS Officer ATO Alternate TAS Officer 								
		AGRE	EMENT					
have read and understood the Policie	s and Guidelines on	the Use of	DPWH Inform	nation and Comm	nunications Technol	ogy (ICT) Resources		
and hereby agree to abide to these; the ICT resources and/or be subjected to o	at any violation ther disciplinary actions.	eof shall lea	ad to the revo	ocation of all my ri	ights and privileges	to access the DPWH		
Employee Name	Signatu	70						
Employee Name	Signata							
			200					
			Attested	d by:				
				Supervisor's S	ignature over Printe	ed Name		
		AUTHOR	IZATION					
	Re	quest Au	thorized by:					
_	7-1	Head o			_			
		a financial and the	Printed Nam		A			
	EVALUATION C	District States of	The second second	ed out by HRAS)				
Pate Received by Human Resource	and Administrat	ive Servic	e:					
Employee Name	Completed T	raining	-	Approval	Re	marks		
	Yes	No	Approved					
	Yes	No No	Approved		The same of the sa			
	Yes	No No	Approved Approved					
	Yes	No	Approved		100			
lecommended by:			Approve	d by:				
					-			
	Application User Coordinator Head of Office (Signature over Printed Name) (Signature over Printed Name)							
(Signature over Fin	No. of Concession, Name of Street, or other Persons, Name of Street, Name of S		C () CD	THE RESERVE OF THE PARTY OF THE	re over Printed Nam	ie)		
	GRANTING O	F ACCES	S (to be filled	out by IMS)				
ate TAS User Access has been gra	ntea:							
	Imple	mented b	ıv:					
					tion Support Persor e over Printed Nam			



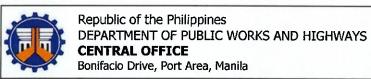
WEB POSTING UTILITY ACCESS REQUEST FORM

Borniacio Drive, i	or Mica, Mail		Service	Rem	lect N	lo.		_			\\/A+L	Ordo	r No.			
			REQ	C. 150			136				VVOIK	Jue	140.	RIT		
			4				100					la la constitución de la constit				
ate of Application:																
ffice/Division/Section:						11500			-	_						
Employee Name (Last Name, First Name Middle Initial)	Employee ID	Network ID								ser G						Others
		CHARLES VAL	ANN	AP	CW	æ	CPE	DIR	GAD	GS	155	REA	LDP	NWS	PPP	(Please spe
			-													
GEND (for User Group)																
- ANN Announcements	• D	IR Director	ע					_	LDP	1.5	NDAD	- ADA				
- AP APP/PMR	• G	AD Gender a	and De	evelo	pmen	t			NWS	Ne	ews					
 CW Civil Works CS Consultancy Services 	• G			vices	;			I	PPP	Pu	ıblic i	Privat	te Par	tners	hip	
 CPE Computer Proficiency Examination 		EA Realignn														
Examination																
	ALIENS TO BE	AC	GREE	ME	NT	300	WB	100	113	719	1000	1,6%	(12)	EA	1/20	Miller Co.
				direction of												
ve read and understood the Po	olicies and Guid	lelines on the L	lse of	DPV	VH In	form	atio	n and	Con	mun	icatio	on Te	chno	loav	(ICT	Reson
I hereby agree to abide by the	ese; that any vi	olation thereof	shall	lead	to t	he r	evoc	ation	of a	II my	righ	ts ar	id pri	vileg	es to	access
VH ICT resources and/or be su	bjected to disc	iplinary actions												_		
Employee Name	ALL ALL FRANCES	Signature	333													
			_													
			_			ttes	ted	hv:								
			_		•		LCU	.								
					-			Linor	vicor	'c Cia	un atu	ro o	or De	inted	Man	
							-	upei	VISOI	2 210	jiiatu	iie ov	ÇI FI	iiiceu	ıwan	ie
		AUTI	HOR	ZAT	TION			Hill		200					0.8	
		Reques	t Aut	hori	zed	bv:										
		•				•										
	_															
		He (Signature)	ad of			ame	١									
		(0191101010	0.0.			um o,	,									
	GRAI	NTING OF AC	CES	S (to	be fi	lled o	out b	y IMS	5)							
te Web Posting Utility User	Access has be	en granted:														
		g-wiitoui							_							
		Imple	ment	ed t	y:											
										licati						
								(Sign	ature	ove	r Prin	ited N	Name	2)	



DATA CHANGE REQUEST FORM

	Editor William	Service Request No REQUEST	Work Order No
Date of Application:			
Name of Application:			
Record ID	Description	Request to	Reason / Correction
	A liming at the con-	Delete Edit	
			Attach additional sheets as necessa
equested by:		Approved by	/ :
Application End House		-	U
Application End-User (Signature over Printed Na	me)		Head of Office (End-User) (Signature over Printed Name)
· 正的是2000年2000年2000年2000年2000年2000年2000年200	EVALUA	ATION OF REQUEST	
n be filled-out by the Application User Coordina oplication End-User	tor if he/she is not the request	ting Evaluated by	
emarks:			
			Application User Coordinator
		***************************************	(Signature over Printed Name)
be filled-out by Information Management Sen	vice		
te Received:		Date Evaluat	:ed:
ction: Approved Disapprovemarks:			
aluated by:			
commended by:		Approved by:	
Chief, Application Support Div	ision	Dire	ector, Information Management Service
(Signature over Printed Nam	ne)		(Signature over Printed Name)
CHIPMON SERVER THE CAPTURE SHAPE SHAPE		TION OF REQUEST	Property and the second
ate Received:		Date Executor	ed:



REQUEST FOR INFORMATION SYSTEMS SERVICES

	Service Request No Work Order No
REC	QUEST (to be filled out by the AUC)
Date Requested:	Name of Application:
Date Required:	Type of Service requested:
Requesting Office:	
Contact Number:	Solospinon (Now / ppilodash)
Contact Number.	Enhancement (Reports, Additional Functionalities / Modules)
Please provide a detailed description of the request. Atta	ach additional documents as necessary.
	·
Note:	
For requests involving reports, please attach a sample format or Office. IMS will not process the request if a sample report is not	f the report (may contain data). The format must be initiated by the AUC and Head of
Sample format attached	. provided.
Sample format acadica	
Requested by:	Approved by:
Application User Coordinator	Head of Office
(Signature Over Printed Name)	(Signature Over Printed Name)
EVALUATIO	ON OF REQUEST (to be filled out by IMS)
Assigned ASP:(Signature over Printed Name)	Date Received by ASP:
Kellark	(S:
Approved	
Disapproved	
Deferred	
Recommended by:	Approved by:
KW4 <u>1.2</u>	
Chief, Application Support Division (Signature over Printed Name)	Director, Information Management Service (Signature over Printed Name)
(Signature over Frinted Name)	(Signature over Printed Name)