



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



097.13 DPWH
b4. 22. 2024

APR 17 2024

DEPARTMENT ORDER)
NO. 58)
Series of 2024)
46 04/22/2024

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

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

In order to ensure that the policies and guidelines on the proper utilization of these resources are aligned with the 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 supersedes the following Department issuances and shall take effect immediately:

1. Department Order No. 13, Series of 2015
2. Department Order No. 24, Series of 2017


MANUEL M. BONOAN
Secretary

11.1.2 RGG/RBC

Department of Public Works and Highways
Office of the Secretary



WIN4P01834

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

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

Revision No. _____
_____, 2024

Table of Contents

| | |
|---|----|
| Acronyms | 4 |
| 1. Purpose..... | 5 |
| 2. Scope..... | 5 |
| 3. Definition of Terms..... | 5 |
| 4. Duties and Responsibilities..... | 7 |
| 4.1. All Users..... | 7 |
| 4.2. Division and Section Chiefs | 7 |
| 4.3. Information Management Service (IMS) and Regional/District IT Support Officers (RITSO/DITSO)..... | 7 |
| 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 |
| 5.3. Monitoring of Compliance | 10 |
| 5.4. Data Security and Accountability | 10 |
| 5.5. Revocation of Privileges..... | 10 |
| 5.6. Sanctions | 10 |
| 6. ICT Equipment..... | 11 |
| 7. Software and Licenses..... | 12 |
| 8. Telephone Service..... | 12 |
| 9. Intranet Service | 13 |
| 9.1. Network Account..... | 13 |
| 9.2. Confidentiality and Security..... | 13 |
| 9.3. Account Lockout | 14 |
| 9.4. Temporary Deactivation of Network Account | 14 |
| 10. Internet Service | 14 |
| 11. VPN Access Service | 15 |
| 12. Email Service | 15 |
| 13. File Storage Service..... | 16 |
| 14. Application Systems | 17 |
| 15. Personally-Owned Devices (PODs)..... | 17 |
| 15.1. Monitoring of Compliance | 17 |
| 15.2. Access Control | 17 |

| | | |
|---------|--|----|
| 15.3. | Security..... | 18 |
| 15.4. | Device Reset and Data Deletion..... | 18 |
| 15.5. | Liability | 19 |
| 15.6. | Services and Support..... | 19 |
| 15.7. | Revocation of Access..... | 19 |
| 16. | General Guidelines | 19 |
| 16.1. | Request for Access to the Department's ICT Services | 19 |
| 16.2. | Request for Access to the Department's Application Systems | 22 |
| 16.3. | Request for VPN Access..... | 23 |
| 16.4. | Accessing Email Platforms..... | 25 |
| 16.4.1. | Standard Email | 25 |
| 16.4.2. | Microsoft Office 365 Email | 25 |
| 16.4.3. | Email Capacity Limits..... | 26 |
| 16.5. | Exchanging Large Files | 26 |
| 16.5.1. | DPWH FileDrop..... | 26 |
| 16.5.2. | OneDrive for Office 365 Users..... | 26 |
| 16.5.3. | SharePoint..... | 26 |
| 17. | Annexes..... | 27 |
| 17.1. | Software and Hardware | 27 |
| 17.1.1. | Network Servers Access Request Form..... | 27 |
| 17.1.2. | Personally-Owned Device (POD) Configuration Request Form | 27 |
| 17.1.3. | Software Installation Request Form | 27 |
| 17.1.4. | Telephone Line and/or Feature Activation Request Form | 27 |
| 17.1.5. | VPN Access Request Form | 27 |
| 17.2. | Intranet, Internet, and Email..... | 27 |
| 17.2.1. | Intranet Access Request Form..... | 27 |
| 17.2.2. | Internet and Email Access Request Form | 27 |
| 17.3. | Application System | 27 |
| 17.3.1. | CEA Access Request Form..... | 27 |
| 17.3.2. | CuSSA Access Request Form | 27 |
| 17.3.3. | CWA User Request Form..... | 27 |
| 17.3.4. | eBudget Access Request Form | 27 |
| 17.3.5. | eNGAS Access Request Form | 27 |
| 17.3.6. | IROWMA Access Request Form | 27 |
| 17.3.7. | MYPS Access Request Form | 27 |
| 17.3.8. | PCMA Access Request Form | 27 |

| | | |
|----------|---|----|
| 17.3.9. | PIS Access Request Form | 27 |
| 17.3.10. | PPMPA Access Request Form..... | 27 |
| 17.3.11. | RBIA Access Request Form | 27 |
| 17.3.12. | RTIA Access Request Form | 27 |
| 17.3.13. | TAS Access Request Form..... | 27 |
| 17.3.14. | Request for Information Systems Services..... | 27 |
| 17.3.15. | Web Posting Utility Access | 27 |
| 17.3.16. | Data Change Request Form..... | 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

- 3.1. Application System - A system to which a computer program or software is applied, such as Civil Works Application (CWA) and Document Tracking System (DoTS).
- 3.2. Bring your own device (BYOD) - A scheme that allows users to bring and use their own computing devices to accomplish work for the DPWH.
- 3.3. 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.
- 3.4. 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.
- 3.5. ICT Resources - The DPWH ICT resources include all hardware and software owned, licensed or by agreement, leased or managed by DPWH, data/files, telephone, intranet, internet, email, and application system.
- 3.6. 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.
- 3.7. 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.

- 3.8. Intranet - A computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization.
- 3.9. Network ID - A string of characters that uniquely identifies a user and allows access to a computer system, communication network and application systems.
- 3.10. Mobile devices - Computing devices that include, but are not limited to, laptop computers, tablet computers, and smartphones.
- 3.11. Peripherals - Any external devices connected to a computer.
- 3.12. Personally-owned device (POD) - A device owned by a user and third parties to produce, modify or view DPWH data.
- 3.13. 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.
- 3.14. 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.
- 3.15. 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.
- 3.16. Spoofing - Faking the sending address of a transmission to gain illegal entry into a secure system.
- 3.17. Virtual Private Network (VPN) - A service that establishes a secure connection between a computing device and a computer network or between two networks.
- 3.18. Work-from-home (WFH) - A work arrangement where government officials or employees work at home or their residence.
- 3.19. 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-DPWH-owned computers and are outside the control of IMS should not use Department-owned/licensed software and must adhere to the Policy on data security provided under Section 5.4 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.

5.3. 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.

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, or its latest issuance.

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 eight 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 ninety (90) 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.

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.

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.

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-DPWH-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.

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.

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:
 - requesting for personal and/or financial information;
 - grammar and spelling errors;
 - sense of urgency or unusual requests;
 - inconsistencies in the email address and links; and
 - contains threats on the alleged recorded malicious activity of the user.
- Suspicious emails should be reported immediately to the IT Service Desk.

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 DPWH-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. The Department will not allow devices that are not compliant with the DPWH Standards for ICT Equipment or represent a threat to the Department's communications network or data.

The IMS shall install and maintain standard configuration of all ICT resources, including personally-owned laptop/notebook computers connecting 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.

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:

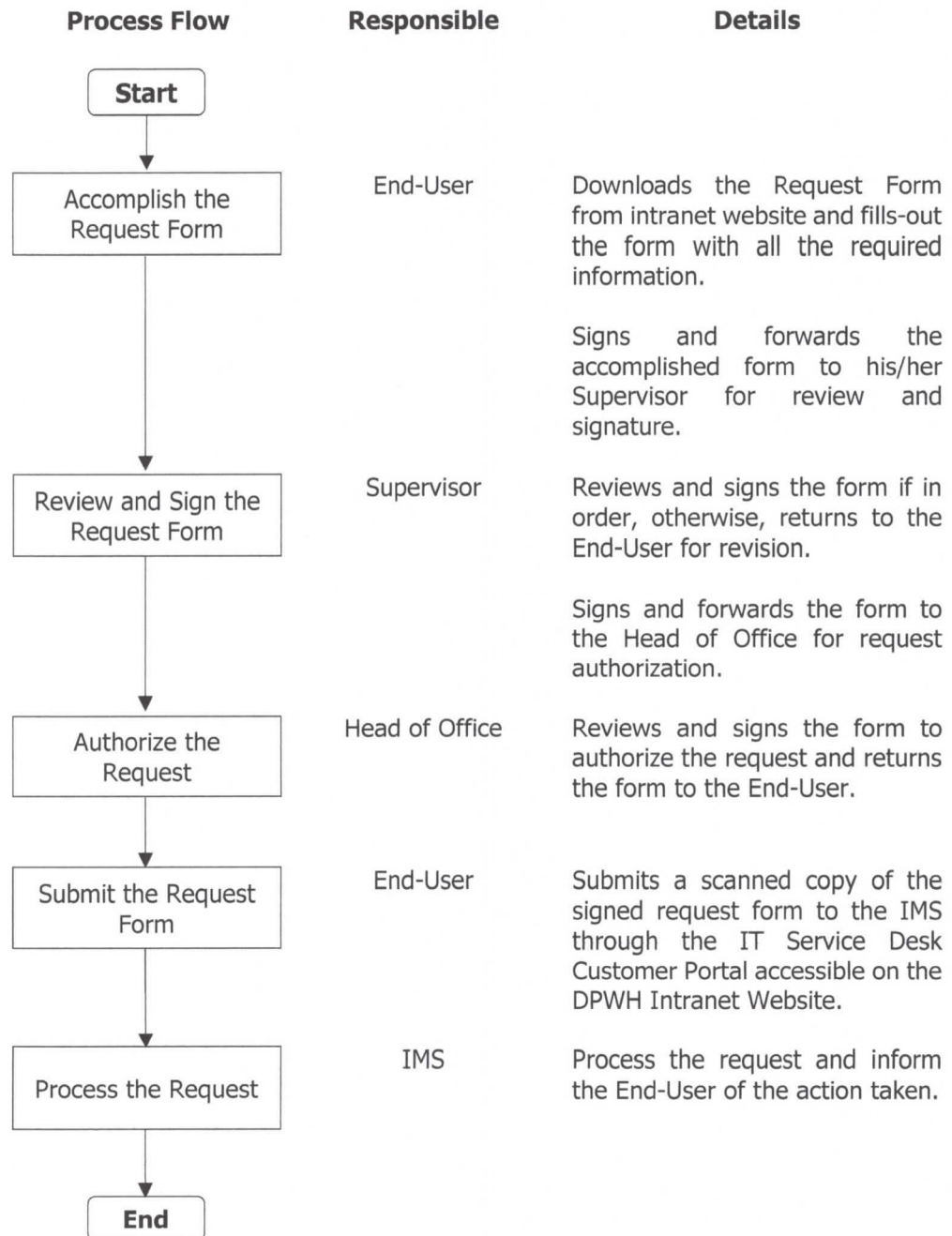
- malware infection or hacking;
- violation of intellectual property rights for the organization's information created, stored, and processed on PODs; and,
- non-compliance with this Policy Guideline.

16. General Guidelines

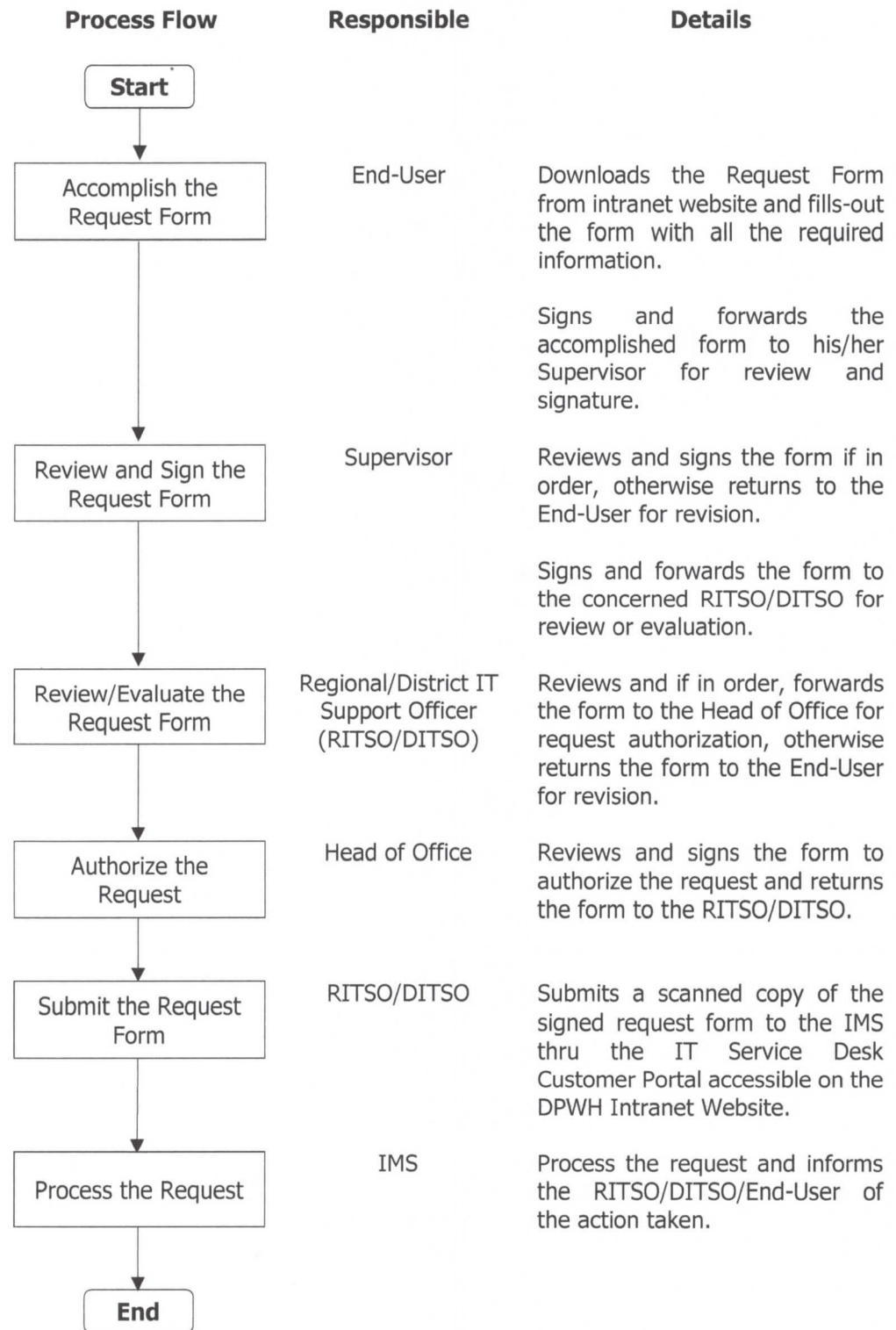
16.1. Request for Access to the Department's ICT Services

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:

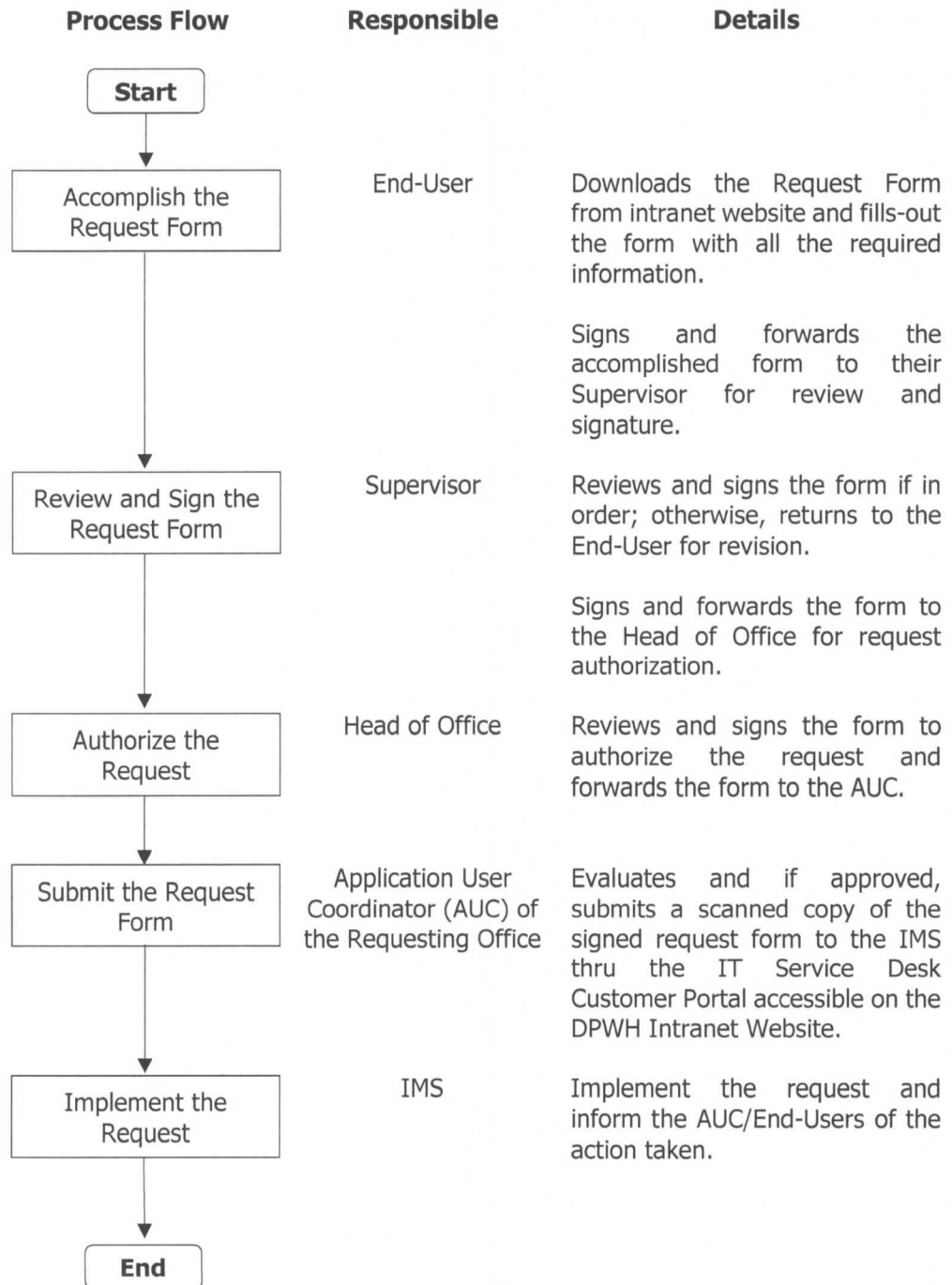


For Regional and District Engineering Offices:



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:



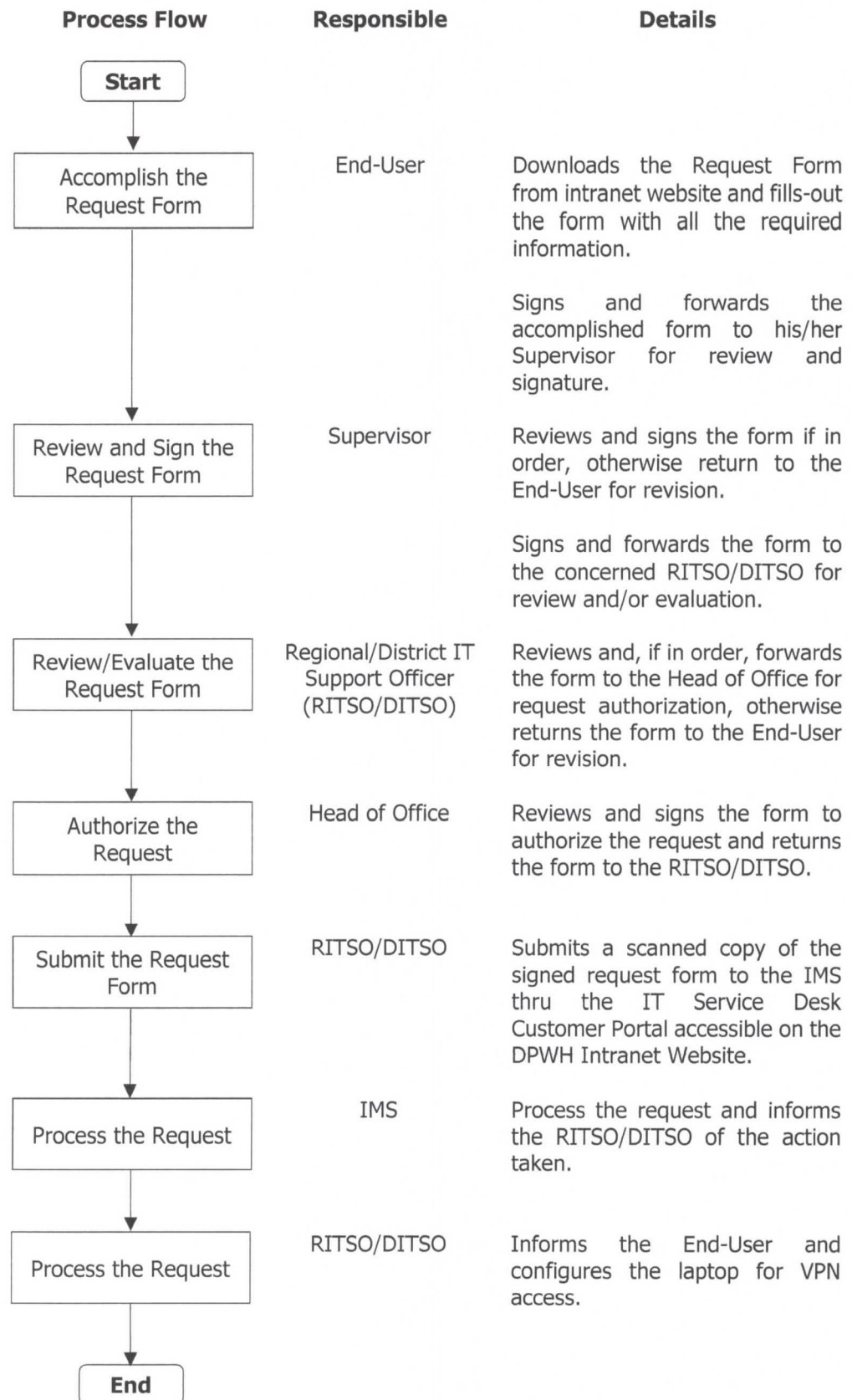
16.3. Request for VPN Access

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:

| Process Flow | Responsible | Details |
|----------------------------------|----------------|--|
| <div>Start</div> | | |
| ↓ | | |
| Accomplish the Request Form | End-User | Downloads the Request Form from intranet website and fills-out the form with all the required information. Signs and forwards the accomplished form to his/her Supervisor for review and signature. |
| ↓ | | |
| Review and Sign the Request Form | Supervisor | Reviews and signs the form if in order, otherwise return to the End-User for revision. Signs and forwards the form to the Head of Office for request authorization. |
| ↓ | | |
| Authorize the Request | Head of Office | Reviews and signs the form to authorize the request and returns the form to the End-User. |
| ↓ | | |
| Submit the Request Form | End-User | Submits a scanned copy of the signed request form to the IMS thru the IT Service Desk Customer Portal accessible on the DPWH Intranet Website. |
| ↓ | | |
| Process the Request | IMS | Process the request and inform the End-User of the action taken. Configures the User’s laptop for VPN access. |
| ↓ | | |
| End | | |

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.

16.4.3. Email Capacity Limits

| 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 Note: this is the standard limit of the majority of the email providers | 30 MB for non-Office 365 recipients 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

- 17.1.1. Network Servers Access Request Form
- 17.1.2. Personally-Owned Device (POD) Configuration Request Form
- 17.1.3. Software Request Form
- 17.1.4. Telephone Line and/or Feature Activation Request Form
- 17.1.5. VPN Access Request Form

17.2. Intranet, Internet, and Email

- 17.2.1. Intranet Access Request Form
- 17.2.2. Internet and Email Access Request Form

17.3. Application System

- 17.3.1. CEA Access Request Form
- 17.3.2. CuSSA Access Request Form
- 17.3.3. CWA Access Request Form
- 17.3.4. DMA Access Request Form
- 17.3.5. eBudget Access Request Form
- 17.3.6. eNGAS Access Request Form
- 17.3.7. IROWMA Access Request Form
- 17.3.8. MYPS Access Request Form
- 17.3.9. PCMA Access Request Form
- 17.3.10. PIS Access Request Form
- 17.3.11. PPMPA Access Request Form
- 17.3.12. RBIA Access Request Form
- 17.3.13. RPS Access Request Form
- 17.3.14. RTIA Access Request Form
- 17.3.15. TAS Access Request Form
- 17.3.16. Web Posting Utility Access Request Form
- 17.3.17. Data Change Request Form
- 17.3.18. Request for Information Systems Services



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

NETWORK SERVERS ACCESS REQUEST FORM

ITSD Incident No.: _____

REQUEST

Date of Application: _____

Office: _____
(Office, Division, Section)

Contact Number (Local): _____

Server Access:

- ☐ Shared folder / data repository
☐ Software / system
☐ Others (specify) _____

Server Machine:

- ☐ Application server
☐ Database server
☐ Web server
☐ Others (specify) _____

Required Server Specifications:

Number of processor: _____
Memory (GB): _____
Disk drives and space (GB): _____
Software: _____

Requested Action: (Please check where applicable)

| Name of Employee | Server / Software / System / Shared Folder Name | Access Rights |
|------------------|---|--|
| | | <input type="checkbox"/> View Only <input type="checkbox"/> Full |
| | | <input type="checkbox"/> View Only <input type="checkbox"/> Full |
| | | <input type="checkbox"/> View Only <input type="checkbox"/> Full |
| | | <input type="checkbox"/> View Only <input type="checkbox"/> Full |
| | | <input type="checkbox"/> View Only <input type="checkbox"/> Full |
| | | <input type="checkbox"/> View Only <input type="checkbox"/> Full |

Purpose:

- ☐ File / data sharing
☐ File / data backup
☐ For information / monitoring
☐ Application development
☐ Software / application testing
☐ Software / application integration
☐ Others (specify) _____

Requested/Authorized by:

Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Name of Employee | Signature | Name of Employee | Signature |
|------------------|-----------|------------------|-----------|
| | | | |
| | | | |
| | | | |

Attested by:

(Supervisor's Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: _____

Date Completed: _____

Action:

- ☐ Approved ☐ Disapproved

Remarks:**Evaluated by:****Recommending Approval:****Approved:**

Chief, Systems Administration Section
(Signature over Printed Name)

Chief, Technology Support Division
(Signature over Printed Name)

Director IV
(Signature over Printed Name)



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

PERSONALLY-OWNED DEVICE (POD) CONFIGURATION REQUEST FORM

ITSD Incident No.: _____

REQUEST

Date of Application: _____ Employment Status: _____
Employee Name: _____
(Last Name, First Name, Middle Name) ☐ Regular Employee
Office: _____ ☐ Casual / Job Order / Trainee
(Office, Division, Section) (Contact expires on _____)
Position: _____ ☐ Consultant / Contractor / Supplier
(Contact expires on _____)
Contact Number (Local): _____

Device Type: ☐ desktop computer ☐ laptop computer ☐ mobile tablet ☐ mobile phone ☐ others _____

Brand and Model: _____ Additional information, if any: _____

Reason:

- ☐ No available DPWH-issued device ☐ The DPWH-issued device is incompatible with the system being accessed
☐ Others _____

Access requirements: ☐ None

- ☐ Internet connection ☐ Email system ☐ Application system (specify) _____
☐ Network printer ☐ Shared file storage ☐ Intranet website ☐ Others _____

AGREEMENT

I acknowledge and agree to the following terms and conditions related to the use of my device for work purposes under the Department's Personally Owned Device program.

I will take reasonable steps to secure my device, such as using a strong password and installing an updated security software. I understand that I am responsible for the security of my device and the Department's data stored on it.

I will ensure that the Department's data stored on my device are protected and secured from unauthorized access. I acknowledge that I am responsible for the backup and recovery of data on my device.

I agree and give full consent for IMS/IT Support Officer to configure my device in accordance with the standards of the Department. I understand that this may involve removal of software that is not consistent with the Department's policies or may pose security risks.

I agree to hold the Department harmless for any damage or losses arising from using my device for work purposes. This includes any liability arising from the loss or theft of my device or any data stored on it.

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

(Employee's Signature over Printed Name)

Attested by:**Requested/Authorized by:**

Supervisor
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: _____

Date Completed: _____

Action:

- ☐ Approved ☐ Disapproved

Remarks:**Evaluated by:****Recommending Approval:****Approved:**

Chief, Systems Administration Section
(Signature over Printed Name)

Chief, Technology Support Division
(Signature over Printed Name)

Director IV
(Signature over Printed Name)



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

SOFTWARE REQUEST FORM

ITSD Incident No.: _____

REQUEST

Date of Application: _____

Office: _____
(Office, Division, Section)

Contact Number (Local): _____

Server Access:

- ☐ Software installation
☐ License use
☐ Others (specify) _____

Specifications:

Requested Action: (Please check where applicable)

| Name of Employee | Software | Version | To be installed on | | |
|------------------|----------|---------|----------------------------------|---------------------------------|---------------------------------|
| | | | <input type="checkbox"/> Desktop | <input type="checkbox"/> Laptop | <input type="checkbox"/> Server |
| | | | <input type="checkbox"/> Desktop | <input type="checkbox"/> Laptop | <input type="checkbox"/> Server |
| | | | <input type="checkbox"/> Desktop | <input type="checkbox"/> Laptop | <input type="checkbox"/> Server |
| | | | <input type="checkbox"/> Desktop | <input type="checkbox"/> Laptop | <input type="checkbox"/> Server |
| | | | <input type="checkbox"/> Desktop | <input type="checkbox"/> Laptop | <input type="checkbox"/> Server |
| | | | <input type="checkbox"/> Desktop | <input type="checkbox"/> Laptop | <input type="checkbox"/> Server |

Purpose:

Requested/Authorized by:

Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Name of Employee | Signature | Name of Employee | Signature |
|------------------|-----------|------------------|-----------|
| | | | |
| | | | |
| | | | |

Attested by:

(Supervisor's Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: _____

Date Completed: _____

Action:

- ☐ Approved ☐ Disapproved

Remarks:

Evaluated by:
Recommending Approval:
Approved:

Chief, Systems Administration Section
(Signature over Printed Name)

Chief, Technology Support Division
(Signature over Printed Name)

Director IV
(Signature over Printed Name)



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

TELEPHONE LINE AND/OR FEATURE ACTIVATION REQUEST FORM

ITSD Incident No.:

REQUEST

Date of Application: _____
Employee Name: _____
(Last Name, First Name, Middle Name)
Office: _____
(Office, Division, Section)
Position: _____
Contact Number (Local): _____

Employment Status:
☐ Regular Employee
☐ Casual / Job Order / Trainee
(Contact expires on _____)
☐ Consultant / Contractor / Supplier
(Contact expires on _____)

Average number of telephone calls:

| Nature | Daily | Weekly | Monthly |
|------------------------------------|-------|--------|---------|
| International | | | |
| National (other than DPWH offices) | | | |
| National (DPWH offices) | | | |

Requested Action: (Please check where applicable)

| Type of Access | Purpose / Reason |
|---|------------------|
| <input type="checkbox"/> Telephone Line | |
| <input type="checkbox"/> Telephone Outlet | |
| <input type="checkbox"/> International Direct Dialing (IDD) | |
| <input type="checkbox"/> National Direct Dialing (NDD) | |

Requested/Authorized by:

Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

Attested by:

(Employee's Signature over Printed Name)

(Supervisor's Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: _____

Date Completed: _____

Purpose: (Please check where applicable)

- ☐ research, procurement, public information, education and training
☐ infrastructure planning, design and construction
☐ calamity and disaster operations
☐ user of the Department's application systems
☐ Others _____

- ☐ downloading/uploading of data from/to external offices/agencies
☐ communication and/or submission of reports with internal/external offices
☐ updating of technical documents and gathering of best practices from different external entities

Action:

☐ Approved ☐ Disapproved

Remarks:

Evaluated by:

Recommending Approval:

Approved:

Chief, Network Administration Section
(Signature over Printed Name)

Chief, Technology Support Division
(Signature over Printed Name)

Director IV
(Signature over Printed Name)



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

VPN ACCESS REQUEST FORM

ITSD Incident No.:

REQUEST

Date of Application: _____
Employee Name: _____
(Last Name, First Name, Middle Name)
Office: _____
(Office, Division, Section)
Position: _____
Contact Number (Local): _____

Employment Status:
☐ Regular Employee
☐ Casual / Job Order / Trainee
(Contact expires on _____)
☐ Consultant / Contractor / Supplier
(Contact expires on _____)

Purpose/Reason

- ☐ WAN connectivity is not available in the office (disconnected)
☐ Requires remote access to office files and/or application systems from home
☐ Consistently doing field work
☐ On vacation leave / study leave / maternity leave until _____
(specify end date)
☐ Others (specify) _____

Requirements

The User has an existing DPWH-issued device to be used for VPN access?
☐ Yes ☐ No

What will be accessed thru VPN?
☐ Office computer and files
☐ Intranet website and issuances
☐ Network file storage
☐ Application system (specify): _____

Requested/Authorized by:

Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

Attested by:

(Employee's Signature over Printed Name)

(Supervisor's Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: _____

Date Completed: _____

Purpose: (Please check where applicable)

- ☐ research, procurement, public information, education and training
☐ infrastructure planning, design and construction
☐ calamity and disaster operations
☐ user of the Department's application systems
☐ Others _____

- ☐ downloading/uploading of data from/to external offices/agencies
☐ communication and/or submission of reports with internal/external offices
☐ updating of technical documents and gathering of best practices from different external entities

Action:

- ☐ Approved: ☐ VPN client (GlobalProtect) ☐ clientless VPN (web portal) ☐ Temp. VPN access
☐ Disapproved

Remarks:

Evaluated by:

Recommending Approval:

Approved:

Chief, Network Administration Section
(Signature over Printed Name)

Chief, Technology Support Division
(Signature over Printed Name)

Director IV
(Signature over Printed Name)



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

INTRANET ACCESS REQUEST FORM

ITSD Incident No.: _____

REQUEST

Date of Application: _____
Employee Name: _____
(Last Name, First Name, Middle Name)
Office: _____
(Office, Division, Section)
Position: _____
Contact Number (Local): _____

Employment Status:
☐ Regular Employee
☐ Casual / Job Order / Trainee
(Contact expires on _____)
☐ Consultant / Contractor / Supplier
(Contact expires on _____)

Note:

Upon approval of the request, the employee shall have access to the DPWH Intranet Website.
For other ICT services, a separate request form shall be submitted.

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

(Employee's Signature over Printed Name)

Attested by:

Supervisor
(Signature over Printed Name)

Requested/Authorized by:

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date Received: _____

Date Completed: _____

DPWH Network ID: _____

Implemented by:

IT Service Desk Analyst
(Signature over Printed Name)



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

INTERNET AND EMAIL ACCESS REQUEST FORM

ITSD Incident No.: _____

REQUEST

Date of Application: _____
Employee Name: _____
(Last Name, First Name, Middle Name)
Office: _____
(Office, Division, Section)
Position: _____
Contact Number (Local): _____

Employment Status:
☐ Regular Employee
☐ Casual / Job Order / Trainee
(Contact expires on _____)
☐ Consultant / Contractor / Supplier
(Contact expires on _____)

Requested Action: (Please check where applicable)

Type of Access

| | |
|--|---|
| <input type="checkbox"/> Access government websites | <input type="checkbox"/> Send email to DPWH Offices |
| <input type="checkbox"/> Access private organizations' websites and online platforms | <input type="checkbox"/> Send email to other government agencies and private org. |
| Purpose/Reason: _____ _____ _____ | Purpose/Reason: _____ _____ _____ |
| Email configuration: | |
| <input type="checkbox"/> Increase maximum number of email recipients | |
| Purpose/Reason: _____ _____ _____ | |
| <input type="checkbox"/> Increase mailbox capacity | |
| Purpose/Reason: _____ _____ _____ | |

Requested/Authorized by:

Head of Office
(Signature over Printed Name)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

Attested by:

(Employee's Signature over Printed Name)

(Supervisor's Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Date Received: _____

Date Completed: _____

Purpose: (Please check where applicable)

- ☐ research, procurement, public information, education and training
☐ infrastructure planning, design and construction
☐ calamity and disaster operations
☐ user of the Department's application systems
☐ Others _____

- ☐ downloading/uploading of data from/to external offices/agencies
☐ communication and/or submission of reports with internal/external offices
☐ updating of technical documents and gathering of best practices from different external entities

Action:

- ☐ Approved: ☐ internet access ☐ government sites access ☐ external email ☐ internal email
☐ increase maximum number of recipients to ____ ☐ increase mailbox size to ____
☐ Disapproved

Evaluated by:

Recommending Approval:

Remarks:

Approved:

Chief, Systems Administration Section
(Signature over Printed Name)

Chief, Technology Support Division
(Signature over Printed Name)

Director IV
(Signature over Printed Name)



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

**COST ESTIMATION APPLICATION
(CEA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | | |
|---|-------------|------------|------------|-----|------|------|------|-------|-------|
| | | | AA | CEM | CETL | CETM | CERM | CERTL | CERTM |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

LEGEND (for User Group)

- **AA** Application Administrator
- **CEM** Cost Estimation Manager
- **CETL** Cost Estimation Team Leader
- **CETM** Cost Estimation Team Member
- **CERM** Cost Estimation Review Manager
- **CERTL** Cost Estimation Review Team Leader
- **CERTM** Cost Estimation Review Team Member

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by BOC)

Date Received by Bureau of Construction: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Approved by:

Application User Coordinator
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date CEA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**CUSTOMER SATISFACTION SURVEY
APPLICATION (CuSSA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | |
|---|-------------|------------|------------|-----|-----|------|------|------|
| | | | AA | SRS | FDO | CPIO | RPIO | DPIO |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

LEGEND (for User Group)

- **AA** Application Administrator
- **SRS** Stakeholders Relations Service User
- **FDO** Front Desk Officer

- **CPIO** Central Office Public Information Officer
- **RPIO** Regional Public Information Officer
- **DPIO** District Public Information Officer

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by SRS)

Date Received by Stakeholders Relations Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Approved by:

Application User Coordinator
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date CuSSA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**CIVIL WORKS APPLICATION
(CWA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | |
|---|-------------|------------|------------|------|----|------|--------|
| | | | SUP | RUIC | VW | UPMO | RO/DEO |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

LEGEND (for User Group)

- **SUP** **Supervisor**
- **RUIC** **Registry Updating & Issuance of CRC**
- **VW** **View for Administrative Personnel**
- **UPMO** **UPMO Coordinator**
- **RO/DEO** **Regional/District Eligibility**

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by PrS)

Date Received by Procurement Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date CWA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**DESIGN MANAGEMENT APPLICATION
(DMA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | | |
|---|-------------|------------|-------------|-----|------|-----|-------------|-------|------|
| | | | Design Team | | | | Review Team | | |
| | | | DM | DTL | DSTL | DTM | RDTL | RDSTL | RDTM |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

LEGEND (for User Group)

- **DM** Design Manager
- **DTL** Design Team Leader
- **DSTL** Design Sub Team Leader
- **DTM** Design Team Member
- **RDTL** Review Design Team Leader
- **RDSTL** Review Design Sub Team Leader
- **RDTM** Review Design Team Member

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by BOD)

Date Received by Bureau of Design: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Approval:

Application User Coordinator
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date DMA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**ELECTRONIC BUDGET SYSTEM
(eBudget) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | |
|---|-------------|------------|------------|----|----|----|----|-----|
| | | | PR | AP | AU | IT | SA | AUC |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

LEGEND (for User Group)

- PR Preparation
- AP Approval
- AU Audit / Read Only

- IT IT Support Officer
- SA System Administrator
- AUC Data Steward / AUC

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by FS)

Date Received by Finance Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date eBudget User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**ELECTRONIC NEW GOVERNMENT
ACCOUNTING SYSTEM (eNGAS) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | |
|---|-------------|------------|------------|----|----|----|----|-----|
| | | | PR | AP | AU | IT | SA | AUC |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

LEGEND (for User Group)

- PR Preparation
- AP Approval
- AU Audit / Read Only

- IT IT Support Officer
- SA System Administrator
- AUC Data Steward / AUC

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by FS)

Date Received by Finance Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date eNGAS User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

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

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | |
|---|-------------|------------|------------|----|----|-----|--------|-------|
| | | | HEAD OF IO | TL | SP | AUC | MANCOM | ADMIN |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

LEGEND (for User Group)

- **HEAD OF IO** Head of Implementing Office
- **TL** ROW Team Leader
- **SP** ROW Specialist
- **AUC** Application User Coordinator
- **MANCOM** Management Committee
- **ADMIN** IROWMA Administrator

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by LS)

Date Received by Legal Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date IROWMA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

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

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | | | | | | |
|---|-------------|------------|------------|-----------|----------|-----------|----------|---------|-----|-----|-----------|-----|-------|
| | | | DPC | DPD Admin | DPD Coor | FAPs Coor | PD Admin | PD Coor | PPC | RPC | Read Only | UPC | ADMIN |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

LEGEND (for User Group)

- **DPC** District Planning Coordinator
- **DPD Admin** Development Planning Division Administrator
- **DPD Coor** Development Planning Division Coordinator
- **FAPs Coor** Foreign Assisted Projects Coordinator
- **PD Admin** Programming Division Administrator
- **PD Coor** Programming Division Coordinator
- **PPC** PIP Planning Coordinator
- **RPC** Regional Planning Coordinator
- **UPC** UPMO Planning Coordinator
- **ADMIN** MYPs Administrator

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by PS)

Date Received by Planning Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date MYPs User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**PROJECT AND CONTRACT MANAGEMENT
APPLICATION (PCMA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | | |
|---|-------------|------------|------------|--------|---------|-----|----|----|----|
| | | | RD/ARD | DE/ADE | CCD/CCS | MoE | PM | PE | PI |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

LEGEND (for User Group)

- RD/ARD Regional Director / Assistant Regional Director
- DE/ADE District Engineer / Assistant District Engineer
- CCD/CCS Chief, Construction Division / Section
- MoE Monitoring Engineer
- PM Project Manager
- PE Project Engineer
- PI Project Inspector

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |
| | |

Attested by: _____

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by: _____

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by BOC)

Date Received by Bureau of Construction: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Approved by: _____

Application User Coordinator
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date PCMA User Access has been granted: _____

Implemented by: _____

Application Support Person
(Signature over Printed Name)



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

**PERSONNEL INFORMATION SYSTEM
(PIS) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | | | | | | | | Module | | | |
|---|-------------|------------|------------|-----|----|-----|----|----|----|----|----|----|-----|----|--------|----|----|----|
| | | | CO | | | | | | | | RO | | DEO | | | | | |
| | | | CDD | EWB | ES | PPS | RM | SU | TO | RO | RA | RO | DA | RO | PL | PD | LV | LB |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |

LEGEND

For User Group

- CDD Capacity Development
- EWB Employee's Welfare & Benefit
- ES Employment Staffing
- PPS PPS Payroll & Personnel Info
- RM Records Management

- SU Super Admin
- TO TAS Officer
- RA Regional Admin
- DA District Admin
- RO Read Only

For Module

- PL Plantilla
- PD Personnel Data
- LV Leave
- LB Library

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by HRAS)

Date Received by Human Resource and Administrative Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date PIS User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**PROJECT PROCUREMENT MANAGEMENT
PLAN APPLICATION (PPMPA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | |
|---|-------------|------------|------------|-----|-----|-----|
| | | | AU | CPA | RPA | DPA |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

LEGEND (for User Group)

- **AU** **Application User**
- **CPA** **Central Procurement Administrator**
- **RPA** **Regional Procurement Administrator**
- **DPA** **District Procurement Administrator**

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources and hereby agree to abide by these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by PrS)

Date Received by Procurement Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approval:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date PPMPA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**ROAD AND BRIDGE INFORMATION
APPLICATION (RBIA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group (Mark only one) | | | | | | | | Data Security Group (Mark only one) | | | |
|---|-------------|------------|----------------------------|----|-----|----|-----|-------|-----|------|--|------|----------------------------|--|
| | | | SU | GL | ICU | RO | BMS | BMS-A | PMS | ARDL | ARDS | ADSD | RO/DEO (Please specify) | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

LEGEND (for User Group)

- SU RBIA Super User
- GL GIS & LRS
- ICU Inventory and Condition Update
- RO Read Only

- BMS Bridge Management System
- BMS-A Bridge Management System Admin
- PMS Pavement Management System

LEGEND (for Data Security Group)

- ARDL All RBIA Data and LRS
- ARDS All RBIA Data and Data Sources
- ADSD All Data (SD Workgroup)

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by PS)

Date Received by Planning Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date RBIA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)

REGULAR PAYROLL SYSTEM (RPS) ACCESS REQUEST FORM

Service Request No. _____ Work Order No. _____

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | Office / Division / Section | User Group | | | |
|---|-------------|------------|-----------------------------|------------|----|----|---|
| | | | | PP | FS | PA | P |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

- PP Payroll Processor
- FS Finance Service/Finance Office User
- PA Payroll Administrator/Team Lead
- P Programmer

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) resources and hereby agree to abide by these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

Request Authorized by:

Head of Office
(Signature over Printed Name)

Date Received by Human Resource Management: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Approval:

Application User Coordinator
(Signature over Printed Name)

Date RPS User Access has been granted:

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**ROAD TRAFFIC INFORMATION
APPLICATION (RTIA) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | |
|---|-------------|------------|------------|----------|---------------------|-------|
| | | | NRTSP COC | NRTSP RC | RO (Please specify) | ADMIN |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

LEGEND (for User Group)

- NRTSP COC NRTSP Central Office Coordinators
- NRTSP RC NRTSP Regional Coordinators
- ADMIN RTIA Administrator

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources and hereby agree to abide to these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by BQS)

Date Received by Bureau of Quality and Safety: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date RTIA User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

**TIME AND ATTENDANCE SYSTEM
(TAS) ACCESS
REQUEST FORM**

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | |
|---|-------------|------------|------------|-----|-----|
| | | | ADMIN | PTO | ATO |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

LEGEND (for User Group)

- **ADMIN** Administrator
- **PTO** Primary TAS Officer
- **ATO** Alternate TAS Officer

AGREEMENT

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 lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

EVALUATION OF REQUEST (to be filled out by HRAS)

Date Received by Human Resource and Administrative Service: _____

| Employee Name | Completed Training | | Approval | | Remarks |
|---------------|------------------------------|-----------------------------|-----------------------------------|--------------------------------------|---------|
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |
| | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> Approved | <input type="checkbox"/> Disapproved | |

Recommended by:

Approved by:

Application User Coordinator
(Signature over Printed Name)

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date TAS User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)



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

WEB POSTING UTILITY ACCESS REQUEST FORM

Service Request No. _____ Work Order No. _____

REQUEST

Date of Application: _____

Office/Division/Section: _____

| Employee Name (Last Name, First Name Middle Initial) | Employee ID | Network ID | User Group | | | | | | | | | | | | | Others (Please specify) |
|---|-------------|------------|------------|----|----|----|-----|-----|-----|----|-----|-----|-----|-----|-----|----------------------------|
| | | | ANN | AP | CW | CS | CPE | DIR | GAD | GS | ISS | REA | LDP | NWS | PPP | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |

LEGEND (for User Group)

- ANN Announcements
- AP APP/PMR
- CW Civil Works
- CS Consultancy Services
- CPE Computer Proficiency Examination
- DIR Directory
- GAD Gender and Development
- GS Goods and Services
- ISS Issuances
- REA Realignment
- LDP LDDAP - ADA
- NWS News
- PPP Public Private Partnership

AGREEMENT

I have read and understood the Policies and Guidelines on the Use of DPWH Information and Communication Technology (ICT) Resources and hereby agree to abide by these; that any violation thereof shall lead to the revocation of all my rights and privileges to access the DPWH ICT resources and/or be subjected to disciplinary actions.

| Employee Name | Signature |
|---------------|-----------|
| | |
| | |
| | |
| | |
| | |

Attested by:

Supervisor's Signature over Printed Name

AUTHORIZATION

Request Authorized by:

Head of Office
(Signature over Printed Name)

GRANTING OF ACCESS (to be filled out by IMS)

Date Web Posting Utility User Access has been granted: _____

Implemented by:

Application Support Person
(Signature over Printed Name)

DATA CHANGE REQUEST FORM

Service Request No. _____ Work Order No. _____

Date of Application: _____

Office/Division/Section: _____

Name of Application: _____

| Record ID | Description | Request to | | Reason / Correction |
|-----------|-------------|------------|------|---------------------------------------|
| | | Delete | Edit | |
| | | | | Attach additional sheets as necessary |

Approved by:

Head of Office (End-User)
(Signature over Printed Name)

To be filled-out by the Application User Coordinator if he/she is not the requesting Application End-User

Evaluated by:

Remarks: _____

Application User Coordinator
(Signature over Printed Name)

To be filled-out by Information Management Service

Date Received: _____

Date Evaluated: _____

Action: ☐ Approved ☐ Disapproved

Remarks: _____

Evaluated by: _____

Recommended by:

Approved by:

Chief, Application Support Division
(Signature over Printed Name)

Director, Information Management Service
(Signature over Printed Name)

Date Received: _____

Date Executed: _____

Remarks: _____

Executed by: _____



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

REQUEST FOR INFORMATION SYSTEMS SERVICES

Service Request No. _____ Work Order No. _____

REQUEST (to be filled out by the AUC)

Date Requested: _____ Name of Application: _____
Date Required: _____ Type of Service requested:
Requesting Office: _____
Contact Number: _____
☐ Development (New Application)
☐ Enhancement (Reports, Additional Functionalities / Modules)

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

Note:

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

☐ Sample format attached

Requested by:

Approved by:

Application User Coordinator
(Signature Over Printed Name)

Head of Office
(Signature Over Printed Name)

EVALUATION OF REQUEST (to be filled out by IMS)

Assigned ASP: _____
(Signature over Printed Name)

Date Received by ASP: _____

Action:

Remarks:

- ☐ Approved
☐ Disapproved
☐ Deferred

Recommended by:

Approved by:

Chief, Application Support Division
(Signature over Printed Name)

Director, Information Management Service
(Signature over Printed Name)