097.13 DPWH
03.21.2007

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

MAR 2 1 2007

DEPARTMENT ORDER)
NO. 20)
Series of 2007 03.21.07)

SUBJECT: **Revised Policies and Guidelines on the Use of DPWH Information Technology Resources, Including Computers, Communication Network, and the Internet**

While the DPWH provides its entitled officials and employees with computers and electronic communications services for the effective performance and fulfillment of their respective job responsibilities, they must, as users, be aware that these services and facilities are for the intent of increasing productivity and for DPWH business purposes only. Users should have no expectation of privacy while using Department-owned or Department-leased equipment. Information passing through or stored on the Department equipment can and will be monitored.

These policies and guidelines are necessary for information security. Therefore, it is important that all IT connections are secured, controlled, and monitored, and that specific policies and guidelines are followed in the use of these services and facilities.

Section 1. Definition of Terms - The acceptable use of information technology is an important concern for all users. For common understanding, the following terms that comprise Information Technology are hereby defined hereunder:

a. hardware - all equipment involved in the operations of a computer system, including, but not limited to, computers, data communications equipment, workstations, and various peripherals such as printers and plotters;

b. software - all programs involved in the operation of a computer system, including, but not limited to, operating systems, data communications software, database management systems and applications software;

c. workstation - any device capable of receiving data from or transmitting data to a computer system;

d. application system - system to which a computer program or software is applied, such as PQ Registry for Civil Works and Contract Preparation System;

e. data file - collection of data accumulated for a definite use, such as Word Processing Documents, Spreadsheets and Databases, etc.

f. network - interconnected set of computer hardware peripherals and devices;

g. intranet - a network system that is used for sharing of network resources within an organization; and,

h. internet - a large computer network linking smaller computer networks worldwide.

Section 2. Scope – The policies and guidelines in this Department Order cover all the hardwares, softwares, systems, programs, the Internet, and all other components of the Department's voice and data communication network, whether these are leased or are acquired on a purchase or on a lease-purchase basis.

This policy is an overall guideline for all technology use. Additional policies that address specific issues such as Hardware Standards, Software Standards, E-mail Use, Equipment Use, Disaster Recovery Plans and Technical Support shall be adopted.

Furthermore, it shall apply to all the offices of the DPWH, i.e., Services, Bureaus, Regional/District Offices, Project Management Offices, Special Committees, Consultants, and other entities.

Section 3. Duties and Responsibilities – The following are the duties and responsibilities of employees, supervisors and the Monitoring and Information Service (MIS) in the implementation of the policies and guidelines for the use of DPWH IT resources:

a. Employees (All Users)

All employees who use DPWH IT resources shall follow the policies and guidelines prescribed herein. Failure to do so may lead to loss of privileges and/or disciplinary action as provided under Section 5 hereof. All IT- related problems should be coursed through the IT Help Desk.

b. Supervisors

All concerned supervisors of employees using DPWH IT resources are responsible for ensuring that their subordinates adhere to the provisions of this Department Order. It is their responsibility to control all activities of their respective staff pertaining to the use of their computers and internet access.

They shall conduct routine inspection/inventory and monitor the use of all DPWH IT resources in their respective areas. They shall report to the MIS any violation of the IT policies and guidelines.

Management of hardwares and softwares is most effective when agency employees are educated concerning the importance of abiding by the terms of the licenses associated with those products as well as the policies and guidelines to be adhered to. Education begins with a new employee during his/her orientation and revisited with all employees on a periodic basis. Therefore, supervisors should continuously educate their respective staff.

c. Monitoring and Information Service (MIS)

MIS shall mandate rules and regulations for the:

i. proper installation of hardware, software and other peripherals to be connected to the IT Infrastructure;
ii. maintenance and security of all network equipment; and,
iii. implementation of a disaster recovery plan when necessary.

MIS is hereby empowered to remove all unauthorized hardwares and/or softwares connected/installed in the DPWH IT Infrastructure and recommend sanctions to employees violating the guidelines under Section 4 of this Department Order.

It shall direct and oversee the Regional and District Network/System Administrators, IT Help Desk Officers/Technicians, and the Regional Application Support Persons. It shall also provide training to these personnel.

Section 4. Guidelines - The following are the general rules for use of DPWH IT resources as stated in MIS Computer Policies, Standards and Guidelines.

User Security

a. Log-in IDs and/or passwords should never be shared with anyone. Anyone who needs and qualifies for access to a computer system can submit a request for his or her own login ID and password. This request will be acted upon in accordance with the Department's normal approval process.

b. User must change his password with regularity. However, the Department may reset password if the necessity calls for it.

Hardware

a. The MIS must authorize the use of specialized hardware other than those provided in the standard equipment.

b. No computer hardware may be installed without the approval of the MIS. This includes the internal cards or other devices within workstations and servers.

c. Only authorized MIS representatives may perform all types of equipment installations, disconnections, modifications, and relocations of ports and cables.

d. 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.

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

Software:

a. Installation or use of unauthorized, non-standard software, including personally owned software, is prohibited. Only software that is licensed to or owned by the Department is to be installed on the Department's computers. It is the Department's policy to abide with all the laws and regulations regarding copyright and intellectual property right.

b. Computer games shall not be played on Department's computers. Computers in the Department are intended for work purposes only.

c. All softwares (package, programs, applications), data, and data files loaded on the DPWH computer systems are the properties of the DPWH. As such, DPWH retains the right to access, copy, and change, alter, modify, destroy, delete or erase any of these properties.

d. Users are not allowed to download any software, either freeware or shareware, from the Internet, unless authorized by the MIS Director. A request form must be accomplished and coursed through the IT Help Desk.

e. Employees are expected to regularly back-up data files that reside on their individual hard disks to avoid irretrievable loss through hardware failure.

f. Employees who own personal computers may use them for work at home. Those who chose to do so should adhere to this Department Order with regard to use of DPWH-owned software or data files. Use of computers and diskettes from external sources introduces the risk that a "computer virus" could infect DPWH microcomputer systems. Data files should be checked by virus detecting software before copying

them back on to the DPWH microcomputers. The MIS shall provide consultation and assistance to avoid this danger.

g. Users are responsible for ensuring that Anti Virus definition is always updated as well as other security patches. They should follow instructions sent through MS Outlook by Network/Systems Administrators.

Data

a. Data should be protected from viruses and secured to prevent theft and alteration.
b. Data must be backed up and be restored as required in the event that a disaster or an interruption occurs during normal operation.

Network Communication and the Internet

a. The Internet connection and E-Mail system of the Department are for official use only. This policy covers services located on any workstations and servers under the jurisdiction and/or ownership of the Department.

   This also applies to computers attached to the network as well as stand-alone workstations with dial-up modems. Account owners are responsible, and shall be held accountable, for any activity performed under their respective IDs and passwords.

b. Computers assigned to officials with the rank of Director III and above will automatically be provided with Internet access. Others may avail or request Internet access at the discretion of their respective Directors or authorized supervisors and the MIS Director.

c. Users shall not use the Department's Internet service to view, download and/or save materials related to any of the following:

   i. offensive content of any kind, including pornographic material;
   ii. promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion or disability;
   iii. threatening or violent behavior;
   iv. illegal activities;
   v. gambling;
   vi. personal financial gain;
   vii. dispensing data to the Department's customers or clients without authorization; and/or,
   viii. opening files received from the Internet without performing a virus scan.

d. The Department forbids the use of its electronic communication resources for any purpose that could strain or compromise these

resources. All electronic mail and data on any DPWH computers may be examined by the authorized representative of the DPWH to determine whether the electronic mail or data contain an inappropriate information or illegal material.

Section 5. Sanctions - Pursuant to the expressed provisions of Section 22 ©, Rule XIV, Book V of Executive Order No. 292, series of 1987, the corresponding penalties for violation of reasonable office rules and regulations are as follows:

a.	1st offense	-	Reprimand
b.	2nd offense	-	Suspension for one (1) to thirty (30) days
c.	3rd offense	-	Dismissal

This Order revokes Department Order No.165, s. 2003 – Policies and Procedures for the Use of Information Technology Resources, Including Computers, Communication Network, and the Internet, and takes effect immediately.

MANUEL M. BONOAN
Officer-In-Charge

WIN7P00082