



Republika ng Pilipinas
KAGAWARAN NG PAGAWAIN AT LANSANGANG PAMBAYAN
TANGGAPAN NG KALIHIM

Maynila

JUN 23 2003

DEPARTMENT ORDER)
NO. **165**)
Series of 2003 *DPWH 06-25-03*

SUBJECT: Policies and Procedures for the
Use of Information Technology
Resources, Including Computers,
Communication Network, and
the Internet (Amendments to
D.O. No. 221, Series of 2000)

While the DPWH provides its users with computers and electronic communications services for the effective performance and fulfillment of job responsibilities, users must be aware of that these services and facilities are for the purpose 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, procedures and guidelines are necessary for information security. Therefore, it is important that all connections be 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. Information Technology is defined as:

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

Section 2. Scope – The policies and procedures in this Department Order cover all the hardware, software, systems, programs, the Internet, and all components of the Department's voice and data communication network, whether these are acquired on a purchase, or a lease/purchase basis.

This policy is an overall guideline for all technology use. Additional policies that address specific issues such as E-mail Use, Software Standards, Hardware Standards, 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, 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 procedures for employee use of DPWH IT resources:

a. Employees

The policies and procedures herein are to be followed by all employees who use DPWH IT resources, and failure to do so may lead to loss of privileges and/or more severe disciplinary action as stated in Section 5.

b. Supervisors

All supervisors of employees who use DPWH IT resources are responsible for ensuring that/their subordinates adhere to this Department Order.

c. Monitoring and Information Service (MIS)

The MIS shall conduct routine inspection/inventory and shall monitor the use of all DPWH IT resources, to ensure that the procedures in this Department Order are adhered to. Any IT related problems should be course through IT Help Desk.

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

User Security

- a. Never share your login ID or password 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 dealt with through the Department's normal approval process.

Hardware

- a. The MIS must authorize use of specialized hardware other than 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. The MIS must perform all equipment installations, disconnections, modifications, and relocations.
- 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 leaving, 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 policy to comply with all laws regarding copyright and intellectual property.
- b. Computer games shall not be played on Department's computers. Computers in the Department are intended for work purposes only.
- c. All software (package, programs, applications), data, and data files residing on the DPWH computer systems are property of the DPWH. The DPWH retains the right to access, copy, change, alter, modify, destroy, delete or erase this property.
- d. Users shall not download software either freeware or shareware from the Internet unless authorized by the MIS.

- 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 wish to 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 and they should follow any instructions send from MS Outlook by Network/Systems Administrators.

Network Communication and the Internet

- a. The Internet connection and E-Mail system of the Department is for official use only. This covers services located on any workstations and servers under the jurisdiction and/or ownership of the Department. They apply 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 passwords.
- b. Computers assigned to officials with rank of Director and above will automatically be provided with Intranet and Internet access. Others may avail or request Internet access at discretion of the Director or supervisor and MIS Director.
- c. Users shall not use the Department's Internet service to view, download or save material related to or including:
 - 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. Dispersing data to the Department's customers or clients without authorization
 - viii. Opening files received from the Internet without performing a virus scan
- d. The Department forbids the use of Department 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 DPWH to determine whether the electronic mail or data contain an inappropriate information or illegal material.

Section 5. Sanctions - Pursuant to the express provisions of Book V of Executive Order 292, Rule XIV, Section 22 letter C, page 53, the corresponding penalties for violation of reasonable office rules and regulations are:

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

This Order supersedes Department Order 221 – Policies and Procedures for the Use of Information Technology Resources, Including Computers, Communication Network, and the Internet dated November 27, 2000, and takes effect immediately.


FLORANTE SORIQUEZ
Acting Secretary