



**COOPERATIVE DEVELOPMENT AUTHORITY**

5th Flr. BenLor Bldg., 1184 Quezon Avenue, Quezon City  
Tel. / Fax No. : (02) 3723814 / 3738905 / 3739950 web : www.cda.gov.ph

**JANUARY 7, 2010**

**MEMORANDUM CIRCULAR NO. 2010-01**  
**Series of 2010**

**SUBJECT : INFORMATION & COMMUNICATION TECHNOLOGY (ICT)  
USAGE AND SECURITY POLICY**

---

**Section I. POLICY STATEMENT**

1. All Information and Communications Technology (ICT) facilities and resources of the Cooperative Development Authority (CDA) are valuable assets and must only be used to perform work-related duties or officially authorized activities.
2. The use of these ICT facilities and resources is a privilege granted by the CDA. All users are directed to use these ICT facilities and services properly within legal and proper boundaries.
3. General Principles in the Proper Use of ICT Resources.
  - a. A user may access only those services and parts of the ICT System that are consistent with his/her duties and responsibilities. The ICT System should be used in accordance with its authorized purpose.
  - b. The following uses and acts, discussed in the following paragraphs, are considered violations in the use of the CDA ICT facilities and network:
    - i. Uses contrary to laws, customs, mores and ethical behavior;
    - ii. Uses for personal benefit, business, or partisan activities;
    - iii. Acts that damage the integrity, reliability, confidentiality, security and efficiency of the ICT System;
    - iv. Acts that encroach on the rights of other users; and,
    - v. Acts that violate privacy.
4. Any offense or violation of this policy will be dealt with according to Philippine laws and the rules and regulations of the Civil Service Commission, and policies, procedures and guidelines of the Authority and its integral annexes.

**Section II. SCOPE OF THE POLICY**

1. **Personnel Covered.** This policy applies to all personnel employed by the CDA and in all its offices nationwide.
2. **Items Covered.** This policy covers the proper use of the ICT facilities and resources if using private equipment in CDA, which includes all ICT equipment, software, data in all formats, accessories, networking facilities and services whether central or remote.

**3. Documents Comprising the Policy.** This Policy document consists of the following:

- a. Main Policy Document Policy statements.
- b. Annex A Definition of Terms.
- c. Annex B Usage Offenses and Equivalent Administrative Offenses

**Section III. DEFINITION OF TERMS**

The Definition of Terms found in Annex A shall be used, and shall be an integral part of the ICT Usage and Security Policy. The Definition of Terms shall be updated from time to time to reflect new equipment and services, and new perspectives in the use of ICT resources.

**Section IV. GENERAL NETWORK ACCESS POLICY**

- 1. **Use of ICT Resources.** Agency network resources are to be used primarily for work-related activities and functions. This is to ensure the effective use of networking priority resources and shall apply to all employees.
- 2. **Exception.** Agency Heads may approve the use of network resources beyond the scope of this access policy under the following conditions:
  - a. The intended use of network resources serves a legitimate Agency interest.
  - b. The intended use of network resources is for educational purposes related to the employee's job function.

**Section V. NETWORK SECURITY MANAGEMENT**

- 1. **Components of the Network.** The network components are the following:
  - a. Monitors, storage devices, modems, network cards, memory chips, keyboard, cables and accessories.
  - b. All computer software: applications, utilities, tools, databases.
  - c. All cabling used to carry voice and data.
  - d. All devices to control the flow of voice and data communication, such as hubs, routers, firewalls, switches, etc.
  - e. All output devices including printers, fax machines, CD writers, etc.
- 2. **Authority to Install, Upgrade, Delete.** The authority and responsibility to install, upgrade or modify any hardware or software rests solely on the CDA-MIS group or personnel authorized by the Agency Head to do so.
  - a. **Software Upgrades.** The following are considered modifications: installing patches provided by the software supplier or downloaded from the internet; installing anti-virus software; installing new versions of the operating system or any office applications, e.g., word-processing or spreadsheet applications.
  - b. **Systems Inspection and Deletions.** The CDA-MIS group or authorized personnel may delete files or softwares that are unauthorized, provided that this deletion or modification is done in the presence of the user or his immediate supervisor.
  - c. **Hardware Maintenance.** The CDA-MIS group or authorized personnel is the only authorized entity to inspect any ICT equipment. Equipment, software or services under warranty may not be altered or inspected by unauthorized personnel.



- d. **Equipment Movements.** The CDA-MIS group or authorized personnel is the only authorized entity to move equipment from one location to another, except for mobile computers such as notebooks, laptops, wireless user devices, etc.
- e. **Authority to Secure Equipment and Services.** The CDA-MIS group or the authorized personnel, has the responsibility to maintain security of internet resources against intrusion and destruction. They are tasked to research security and disaster recovery matters to maintain a high degree of reliability of the systems.

## **Section VI. SYSTEM ACCESS REQUIREMENTS**

1. **Access Privilege.** All qualified users of the CDA ICT facilities shall be issued a unique log-in name and password to gain access to network resources.
2. **Passwords.**
  - a. **Confidentiality.** It is the responsibility of the employee to ensure that his/her password remains secret. The employee may not share it with other individuals. The exception is when an employee, for legitimate reasons, surrenders his/her password in the presence of his/her direct supervisor.
  - b. **Standards.** Passwords are to be at a minimum of eight (8) alphanumeric characters. Passwords should not consist of common words or variations on the employee's name, login name, server name, or agency name.
  - c. **Maintenance.** Each user is encouraged to periodically change his/her password in order to have a secured network environment, although the employee has the option to retain his/her password or not when prompted.
3. **Username.** The CDA-MIS group shall issue the standardized naming convention and format of usernames to be adopted.
4. **Security Responsibility.** The Agency reserves the right to hold the employee liable for damages caused by the employee's failure to protect the confidentiality of his of her password in accordance with the above guidelines.
5. **Limits of Use.**
  - a. **Time of Connection.** Access to network resources is available from 8:00 A.M. to 5:00 P.M. daily.
  - b. **Availability.** The CDA-MIS group shall ensure 100% uptime for connection to network services between 8:00 A.M. to 5:00 P.M.

## **Section VII. REMOTE NETWORK ACCESS**

1. **Remote Access Privileges.** When the infrastructure and resources are available, the CDA shall provide remote connection to the CDA Databases and email accounts through the CDA web-portal. Access to the CDA web portal will be on a 24/7 basis, and maintained by CDA MIS Group subject to the following conditions:
2. **Limits of Use.**
  - a. **Time of Connection.** Remote services shall be available for the above-mentioned services from 6:00 P.M. to 7:00 A.M. daily.
  - b. **User-provided Equipment.** The user shall be responsible for providing the computer, modem and phone line, all other accessories and internet to connect to the CDA remote access services.

- c. **User Account and Password.** Users shall be provided a user account and password to connect to the remote services. It is the responsibility of the user to keep this user account and password confidential, and to keep all information regarding remote network access confidential. Propagating remote access details is considered a security breach and grounds for immediate dismissal.

#### **Section VIII. VIRUS PREVENTION**

1. **Authorized Anti-Virus Program.** No anti-virus programs are allowed to be installed in any CDA computer, whether stand-alone or networked, except those prescribed by the CDA-MIS group or the network personnel authorized by the Agency Head.
2. **Installation.** Users may install these anti-virus programs subject to instructions, which shall be made available by the CDA-MIS group or the authorized personnel. The installation can be made through the network.
3. **Announcements and Updates.** The CDA-MIS group is responsible for the daily updating of the anti-virus program located in the servers. The CDA-MIS group shall periodically give advisories to all CDA users to keep them informed of the best practices to combat viruses.
4. **User Responsibility in Anti-Virus Protection.** It is the responsibility of the user to keep his/her anti-virus updated every week.

#### **Section IX. E-MAIL ACCOUNTS**

1. **CDA E-mail Privileges.** The CDA may grant e-mail accounts to designated officials or employees, subject to the following conditions:
  - a. The employee may not use e-mail for purposes that are illegal, immoral, or disallowed by the CDA.
  - b. The e-mail disk space per user is limited to 20Mbytes. It is the responsibility of the user to maintain his e-mail files, i.e., to delete unwanted files, and to save those that are required for archiving.
  - c. Attachments to sent mail should be limited to 1 Mbyte per message.
2. **Responsibility of Maintenance.** The CDA-MIS group shall be responsible for providing email privileges.
3. **Other E-mail Accounts.** The user may use non-CDA e-mail services provided that he/she uses appropriate, non-obscene email usernames, and that the use of these mail services are consistent with the duties and responsibilities of the employee.
4. **Surrender and Waiver.** It is understood that e-mail privileges including the disk files containing the e-mail files of the user are surrendered upon separation, termination, or other circumstances deemed legal by the CDA.

#### **Section X. PRIVACY AND LOGGING**

1. **Ownership and Right to Monitor.** All corporate ICT resources are owned by CDA. The Agency reserves the right to monitor and/or log all network-based activity. The employee is responsible for surrendering all passwords, files, and/or other required resources if requested to do so in the presence of his or her direct supervisor.
2. **Implied User Agreement to Terms and Conditions.** By logging-in to the CDA ICT facilities, the user agrees to the terms and conditions of this Policy.



## **Section XI. USER RESPONSIBILITIES**

1. **Reporting of Troubles or Problems / User Cooperation.** Users should report suspected abuse, especially any damage to, or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions. Users should cooperate with system administrators in any investigation of system abuse.
2. **Contact Person or Unit.** Exception and trouble reports must be made to the CDA-MIS group so that appropriate action can be taken to solve the problem.

## **Section XII. PROHIBITED ACTS AND USES OF THE ICT RESOURCES**

### **1. Uses Contrary to Laws, Customs, Mores, and Ethical Behavior**

- a. **Criminal Use.** Users should not use the CDA Network Information resources for criminal and / or immoral activities.
- b. **Use of Copyrighted material.** Prohibited acts include but are not limited to:
  - i. Copying, reproduction, dissemination, distribution, use, importation, removal, alteration, substitution, modification, storage, unloading, downloading, communication, publication or broadcasting of copyrighted material. Users should properly attribute any material they copy from or through the ICT System.
  - ii. Infringement of intellectual property rights belonging to others through the use of telecommunications networks, which is a criminal offense under Section 33(b) of the Electronic Commerce Act.
- c. **Cheating.** Prohibited acts include but are not limited to:
  - i. Copying a computer file that contains another person's work and submitting it for one's own credit, or, using it as a model for one's own work, without the permission of the owner or author of the work;
  - ii. Submitting the shared file, or a modification thereof, as one's individual work when the work is a collaborative work, or part of a larger project.

### **2. Uses for Personal Benefit, Business or Partisan Activities**

- a. **Commercial Use.** Use of the ICT System for commercial purposes, and product advertisement, for personal profit, unless permitted under other written Office policies or with the written approval of a competent authority.
- b. **Use of the ICT System for any partisan political activities.** Use of ICT resources for religious or political lobbying, for disseminating information or gathering support or contributions for social, political or cause-oriented group, which are inconsistent with the activities of the Agency of the Department.
- c. **Games and Entertainment.** Use of ICT resources to play games, watch video, or any activity unrelated or inappropriate to the duties and responsibilities of the user, especially during office hours.

### **3. Acts that Damage the Integrity, Reliability, Confidentiality and Efficiency of the ICT System.**

- a. Destruction, deletion, removal, modification, or installation of any computer equipment, peripheral, operating system, disk partition, software, database, or other component of the ICT System;

- b. Connection of any computer unit or external network to the ICT System without the permission of the CDA-MIS group or the Agency Head.
- c. Acts that attempt to crash, tie up, or deny any service on the ICT System, such as, but not limited to the following: sending of repetitive requests for the same service (denial of service); sending bulk mail; sending mail with very large attachments; sending data packets that serve to flood the network bandwidth.
- d. Concealment, deletion, or modification of data or records pertaining to access to the ICT System at the time of access, or alter system logs after such access for the purpose of concealing identity or to hide unauthorized use.
- e. Concealment of identity, or masquerading as other users when accessing, sending, receiving, processing or storing through or on the ICT System.

#### 4. Acts that Encroach on the Rights of Other Users

- a. ***Sending Unsolicited E-mail.*** Sending unsolicited mail such as chain-letters, advertisements, jokes, trivia, announcements to non-official groups or activities, offers, inquiries, and the like (spamming);
- b. ***Morally Offensive and Obscene Use.*** Accessing, downloading, producing, disseminating, or displaying material that could be considered offensive, pornographic, racially abusive, culturally insensitive, or libelous in nature.
- c. ***Sending Fraudulent and Harassing Messages.*** Sending messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of the CDA.
- d. ***Acts that interfere with or disrupt other computer users*** such as, but not limited to the following: sending messages through pop-up screens; running programs that simulate crashes; running spyware to monitor activities of other users.

#### 5. Acts which Violate Privacy

In accordance with Republic Act 8792 known as the "Electronic Commerce Act" specifically section 33 A and B the following are prohibited:

##### a. Hacking, Spying or Snooping.

- i. Accessing, or attempting to gain access to archives or systems that contain, process, or transmit confidential information. Authorized users should not exceed their approved levels of access, nor should they disclose confidential information to others.
- ii. Decrypting, attempting to decrypt, or enabling others to decrypt such information, which are intentionally decrypted, password-protected, or secured. Encrypted data are considered confidential, and include, but not limited to: passwords, digital keys and signatures.
- iii. Re-routing or capture of data transmitted over the ICT System.
- iv. Accessing, or attempting to access, restricted portions of the system, such as e-mail lists, confidential files, password-protected files, or files that the user has no authorization to open or browse.

##### b. Unauthorized Disclosure.

- i. Copying, modification, dissemination, or use of confidential information such as, but not limited to: mailing lists; employee directories of any sort; CDA operations data;



research materials, in whole or in part, without the permission of the person or body entitled to give it.

- ii. Searching, or providing copies of, or modifications to, files, programs, or passwords belonging to other users, without the permission of the owners of the said files, programs or passwords.
- iii. Publication on mailing lists, bulletin boards, and the World Wide Web (www), or dissemination of prohibited materials over, or store of such information on, the ICT System. Prohibited materials under this provision include but are not limited to the following:
  1. Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;
  2. Any material that enables others to gain unauthorized access to a computer system. This may include instructions for gaining such access, computer code, or other devices. This would effectively preclude displaying items such as "Hackers Guides", etc.;
  3. Any material that permits an unauthorized user, who has gained access to a system, to carry out any modification of the computer programs or data stored in the system; and
  4. Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system.

#### **6. Acts that Waste Resources**

- a. Printing excess copies of documents, files, data, or programs.
- b. Repeated posting of the same message to as many newsgroups or mailing lists as possible, whether or not the message is germane to the stated topic of the newsgroups or mailing lists targeted.
- c. Sending large unwanted files to a single email address.

#### **Section XIII. TOLERATED USE**

1. **Tolerated Use.** Some ICT use, though unofficial, may be tolerated. These are considered privileges that may be revoked at any time. They include:
  - a. The use of email for personal communication;
  - b. The use of instant messaging applications; and,
  - c. The use of computers to play compressed audio files or audio CDs.
2. **Update to "Tolerated Uses" of ICT Facilities.** The CDA management from time to time may issue a list classifying certain types of use under the category of "Tolerated Use". This list shall form part of this Policy and will be considered binding on all users.

#### **Section XIV. DISCIPLINARY ACTION**

1. **Violations.** Improper use of ICT resources is subject to penalties. The Agency Head, upon the recommendation of the investigative body, may impose preventive suspension to the Internet and network privileges of the offender/suspected violator.

2. **Applicable Laws.** All Disciplinary Action proceedings shall follow the Civil Service Commission Uniform Rules and Regulations on Administrative cases, and/or legal action provided by applicable Philippine laws.
3. **Penalties for Non-CDA Personnel.** Any non-CDA personnel found guilty violating any of the provisions set forth in this Policy, will be barred from entering any CDA premises. The employee who gave permission to the visitor to access the CDA network will also be held liable for all the violations that the visitor may commit.
4. **Penalties.** In addition to the filing of an Administrative case and sanctions against the violators, appropriate charges will be filed in court if offenses are punishable under the E-commerce Law or any other applicable Philippine Laws.

## **Section XV. ENFORCEMENT PROCEDURES**

1. **Implementing Body.** The designated group in the CDA Central Office and CDA regional offices for implementation, monitoring and imposition of penalties for this policy, should include personnel from the CDA-MIS group and from the Human Resources unit.
2. **Jurisdiction of the Implementing Body on Investigation.**
  - a. Upon receipt of a report or complaint of misuse, the implementing body shall conduct an investigation on the matter.
  - b. This group shall have the following authority:
    - i. To summon the subject of the complaint to provide information;
    - ii. To call and interview potential witnesses;
    - iii. To inspect the user's files, diskettes, tapes, e-mail account and/or other computer-accessible storage media, or authorize systems administrators to perform this inspection under its supervision;
    - iv. To retain, as evidence, copies of user files or other data that may be relevant to an on-going investigation, and;
    - v. To extend the suspension or restriction of a user's computing privileges for the duration of the investigation, or as may be deemed necessary to preserve evidence and protect the system and its users.
  - c. The implementing body shall submit the results and recommendations to the Agency Head for appropriate action.
3. **Appropriate Action.** If the implementing body has substantial, sufficient evidence of misuse of ICT resources, and if that evidence points to the computing activities or the computer files of an individual, the Agency Head shall pursue appropriate actions as provided for in the Uniform Rules on Administrative Cases in the Civil Service (CSC Resolutions No. 99-1936).
4. **Filing of Charges.** In cases where there is evidence of serious misconduct or possible criminal activity, appropriate charges shall be filed by the Agency Head to the proper authorities. This, however, does not prohibit any aggrieved party or complainant other than the Agency Head from instituting the filing of charges with the appropriate authorities.
5. **External Legal Processes.** The CDA Network does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, CDA may be required by law to provide electronic or other records or other information related to those records or relating to the use of



information resources. Use of the CDA computer resources and network is granted subject to existing Philippine laws and regulations.

**Section XVI. WAIVER AND DISCLAIMER**


1. **Disclaimer.** While the CDA takes careful steps to provide reliable and professional services in its network, CDA does not guarantee, nor does it provide any warranties, as to the operating characteristics of its ICT resources and facilities to any of its users.
2. **Waiver.** CDA shall not be responsible for any loss or damage, whether direct or indirect, implied or otherwise, that may arise from the use of the CDA ICT facilities and resources by any person or entity.

**Section XVII. EFFECTIVITY**

1. **Effectivity.** This policy is effective upon the approval of the Board of Administrators.
2. **Amendments.** The Authority may amend or modify this policy to maintain the applicability of the policy. These amendments or modifications shall form part of the overall CDA ICT Network and Security Usage Policy, and will be considered binding on all users

This Memorandum Circular approved under BOA Resolution No. 292, Series of 2009 takes effect immediately.

By Authority of the Board of Administrators

  
**LECIRA M. JUAREZ**  
Chairperson