GUIDELINES ON THE USE OF COA INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) RESOURCES -

FOR USERS IN GENERAL

REPUBLIC OF THE PHILIPPINES
COMMISSION ON AUDIT
Commonwealth Avenue, Quezon City
ADMINISTRATION SECTOR
INFORMATION TECHNOLOGY OFFICE

MEMORANDUM

No: AS ITO 2013 - 001

Date: JUL 15 2013

FOR : All Assistant Commissioners, Directors/ Cluster Directors, Heads of Offices, Division/Service Chiefs, and all others concerned
This Commission

SUBJECT : Issuance of Information and Communications Technology (ICT) Guidelines on the Proper Use of ICT Resources

To best serve the interest of the Commission and to ensure consistent and effective discharge of responsibilities through the use of ICT and achieve information security, attached is the ICT Guidelines on the Proper Use of ICT Resources for ICT users in general.

For your information and guidance.

ARCADIO B. CUENCO, JR.
Assistant Commissioner

Table of Contents

I. Guidelines on the Use of COA Information and Communications Technology (ICT) Resources for Users in General

The use of ICT has become an integral and accepted part of our day-to-day tasks in the Commission. ICT is increasing in importance on the operations and it is expected that this trend will continue, to the extent that it becomes a functional requirement not only for the users within the organization but for external users and the public as well.

ICT includes the range of hardware devices, software and applications such as personal computers, assistive technology, scanners, multimedia device and programs, image editing software, database and audit tools/spreadsheet programs. It also includes the communications equipment and the network infrastructure through which employees and other interested users seek and access information including the internet, email and other related services.

COA regards information as a highly valuable asset and is committed to provide a secure IT infrastructure that protects the integrity and confidentiality of information while maintaining its availability and compliance to policy shift towards openness in access to government information. The Guidelines on the Use of COA ICT Resources for Users is primordial in the protection of information from a wide range of threats that may result in the manipulation or loss of data or information. These are designed to establish the users' responsibilities on the proper use of ICT resources so that every employee becomes skilled, confident and informed users.

To best serve the interest of the Commission and to ensure consistent and effective discharge of responsibilities through the maximize use of ICT and achieve information security, the following guidelines on the use of COA ICT resources shall be observed:

SCOPE

These guidelines shall be applicable to all COA officials, employees and all users authorized to access the Commission's technology resources, including permanent and temporary employees or third party personnel such as consultants, contractors and other parties. These Guidelines shall cover the following:

1. User Registration
2. Password management
3. E-mail usage
4. Internet usage
5. Protection against viruses
6. Proper use and maintenance of desktop/laptop computers and other ICT equipment
7. Creating a safe workspace to avoid strain and injury

1. User Registration

Access to information is controlled through a formal user registration process. Each user is identified by a unique User ID so that users can be linked to and made responsible for their actions.

Scope

These guidelines shall be applicable to new user accounts or access to shared information or network devices. Such information can be held within a database, application or share file space.

Specific Guidelines:

1.1 ***New Users***

1.1.1 All new requests for creation of User Account shall be made in writing using the Access Request Form (ITO Form No. 01)
1.1.2 The COA Creation of User Account Request Form shall be accomplished, approved and authorized by the Cluster/Office Director or his designated alternate and forwarded to the Information Technology Office (ITO).
1.1.3 Only COA- owned computers will be assigned a user account.
1.1.4 Users can only login to their assigned computers except for those who were given MS Outlook Web Access.
1.1.5 In cases where there are no available computers and due to the exigency of service, personally-owned computer may be configured to have an account provided that the request shall be approved by the Chairperson. Such request shall state the purpose and duration of access related to training/project or special task.
1.1.6 The logon ID shall follow an internal naming convention. The first letters of the first and middle names followed by the surname, e.g. Ramon Reyes Cruz, the logon ID shall be rrcruz@coa.gov.ph.
1.1.7 The assignment of a temporary password for newly created user account shall be the responsibility of the designated ITO Administrator.
1.1.8 Temporary password shall be unique to an individual and should not be guessable.

2. **Password Management**

The purpose of the User's Identification and Password guidelines is to protect the Commission's information assets from unauthorized use, and possible accidental or intentional misuse, through weak password security practice. At a minimum, all system access shall be authenticated by passwords.

Scope

The scope of this guideline includes all users. Users are defined as anyone with authorized access to the Commission's technology resources, including permanent and temporary employees or third party personnel such as consultants, contractors, and other parties with valid access accounts.

Specific Guidelines

2.1 Upon the approval by the authorized officials of the User Access Request Form (ITO Form No. 01), a temporary password is issued to the requesting personnel. User shall acknowledge the receipt of temporary password.

2.2 The length of a password shall be at least 6-digits and consists of a combination of alphanumeric characters.

2.3 Users shall change all temporary and system generated passwords upon first logon. This applies both to passwords that are attached to a new user account and passwords that have been reset by SAS, ITO. The system will require and prompt for changes upon first logon.

2.4 The system shall enforce regular password changes every 180 days and the users are notified before the password expiration date.

2.5 The system shall maintain a history of previously used passwords and their re-use is prohibited for the last three passwords.

2.6 Users are locked out of their account after three failed logon attempts. Failed logon attempts are the result of attempting to logon using either a faulty logon ID (user name) or password. Log for failed logon attempts shall be subjected for review, investigation, if necessary.

2.7 Passwords shall not be particularly identifiable with the user (such as names of family members, pets, hobbies, or personal interests, etc.)

2.8 It is the responsibility of the user to remember his/her password.

2.9 There are several practices that are considered potentially dangerous to the user's system or entire network. Prohibited password security activities include, but are not limited to:

2.9.1 Revealing or sharing passwords over the phone or to anyone;
2.9.2 Sharing passwords with family members;
2.9.3 Revealing passwords in an e-mail message;
2.9.4 Revealing passwords to an administrative supervisor;
2.9.5 Talking about passwords in front of others;
2.9.6 Creating passwords at the Commission that are the same as passwords used for personal accounts;
2.9.7 Hinting at the format of a password (for example, "my family name")
2.9.8 Revealing passwords to co-workers while on vacation or on leave of absence;
2.9.9 Using the "Remember Password" feature within applications (for example, those available in Outlook Express, Internet Explorer, or Netscape Messenger);
2.9.10 Writing passwords down; and
2.9.11 Storing passwords in a file on any computer form without using encryption.

3. **Electronic Mail (E-Mail) Usage**

The e-mail usage guidelines have been developed to outline acceptable and unacceptable practices in the use of e-mail in the Commission and to assist users in making the most productive use of e-mail in their work.

E-mail is a critical tool in supporting the functions of the Commission that provides for a fast and effective means of communication. The protection of the Commission's information and communications systems is an essential priority.

Scope

This guideline applies to all users authorized to access the Commission's technology resources and the scope includes the rules and limitations governing e-mail use.

Specific Guidelines

3.1 All e-mail accessed by the users while using the Commission's e-mail resources is the property of the Commission and is subject to monitoring, inspection, storage.

3.2 Users shall not transmit, forward, or post internal e-mails or attach internal documents containing sensitive information to anyone outside the Commission.

3.3 Users shall not forward, or post e-mails containing computer virus, worms, Trojan Horses or any other form of malware that could damage or interfere with Commission's network or another user's computer. Immediately delete e-mail or attachment to e-mail that contain virus or suspected to be infected by viruses.

3.4 Users shall refrain from transmitting, forwarding or posting chain letters.

3.5 Users shall not use the e-mail for solicitation, promotion, election related campaign and other non-work related messages.

3.6 Users shall not transmit, forward or post obscene, profane, or offensive materials.

3.7 E-mails received from unknown sources shall be immediately deleted.

4. **Internet Usage**

Misuse and abuse of the internet and the World Wide Web (www) result in network instability, security breaches or other serious problems. Internet usage guidelines shall provide users with rules governing the use of internet, web browsers, and other applications with the ability to access or transfer data to or from servers connected to the internet.

The purpose of this guideline is to define both appropriate and inappropriate use of the internet and web access. The Commission uses security software applications to help screen inappropriate web sites and block users from accessing unauthorized sites.

Scope

These guidelines shall include the use of internet, web browsers, and other applications with the ability to access or transfer data to or from servers connected to the Internet. These also cover the rules and limitations governing their use and enforcement.

Specific Guidelines

4.1 Internet access shall be limited to job related activities that might include:

- 4.1.1 Communication between employees and non-employees for official purposes;
- 4.1.2 IT technical support downloading software upgrades and patches;
- 4.1.3 Review of possible vendor web sites for product information;
- 4.1.4 Reference regulatory or technical information; and
- 4.1.5 Research

4.2 Internet prohibited activities are the following but not limited to:

- 4.2.1 Access to sites that contain obscene, hateful, pornographic, unlawful violent or otherwise illegal material
- 4.2.2 Sending or posting discriminatory, harassing or threatening messages or images on the Internet
- 4.2.3 Using computers to perpetrate any form of fraud and/or software, film or music piracy
- 4.2.4 Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- 4.2.5 Any interaction with UseNet groups, newsgroups, or other topic-based forums on the Internet, or with any Web sites providing material that:
  - Diminishes network performance (streaming media content, online games, and so on)
  - Provides "chat room" services that allow, provide, condone or support online conversations
- 4.2.6 Any interaction with sites or downloading materials that can:
  - Cause network problems
  - Compromise network security

4.3 Users shall bear in mind that their internet activities are monitored and logged.

5. Protection Against Viruses

It is the responsibility of everyone who uses the computer network to take reasonable measures to protect that network from virus infections.

Computer viruses continue to be a threat especially Microsoft Word and Excel macro viruses, which have proved to be extremely problematic. It is every employee's responsibility to take the appropriate precautions to prevent the spread of viruses.

Scope

This guideline outlines the procedures for preventing and managing virus outbreaks. Educate the users about their roles and responsibilities in preventing virus outbreaks. It outlines how various viruses can infect the Commission's network, how the Commission will prevent and/or minimize infections and how the users should respond if they suspect one has infected by the virus.

Specific Guidelines

5.1 How viruses can infect the network

There are three types of computer viruses: true viruses, Trojan horses and worms. True viruses hide themselves, often as macros, within other files, such as spreadsheets or word documents. When an infected file is opened from the computer connected to the network, the virus can spread throughout the network and may do damage. A Trojan horse is an actual program file that, once executed, doesn't spread but can damage the computer in which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

Viruses can enter the network in a variety of ways:

5.1.1 E-mail – Most viruses are sent as an e-mail attachment. These attachments could be documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect the network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.

5.1.2 Disk, CD, Zip disk or other media – Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another file type.

5.1.3 Software downloaded from the Internet – Downloading software via the Internet can also be a source of infection.

5.1.4 Instant messaging attachments – Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software.

5.2 How to prevent and/or minimize virus infection

5.2.1 All internet traffic coming to and going from the network must pass through the Commission's servers and other network devices. Only specific types of network traffic are allowed beyond the organization's exterior firewalls.
For example, an e-mail message that originates outside of the network must pass through the firewall before it is allowed to enter the e-mail server. This device routes suspicious e-mail and attachments to an isolated storage device, defeating the purpose of a virus.

5.2.2 All vulnerable servers run antivirus scanning software that scans our file-sharing data stores, looking for suspicious code.

5.2.3 Every morning, the firewall and server virus scanning programs check for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated, and then the system administrator is informed. When end users turn on their computers at the beginning of the workday, the workstation virus protection program checks with the Commission's server on the network for updates.

5.2.4 The user will then install the update manually by clicking the shortcut icon in your desktop or in the absence of an icon perform the following:

- Windows XP
  - Go to Windows Explorer, My Network Places
  - Type \\ and select coaw2k3dc01
  - Select NAV
  - Choose the latest antivirus software
- Windows 7
  - G to Windows Explorer, Network
  - Type \\ and select coaw2k3dc01
  - Select NAV
  - Choose the latest antivirus software

5.3 Do not open unexpected e-mail attachments, even from co-workers.

5.4 Never open an e-mail or instant messaging attachment from an unknown or suspicious source.

5.5 Never download freeware or shareware from the Internet without permission from ITO.

5.6 If a file you receive contains macros that are unsure about, disable the macros.

5.7 Regularly update your antivirus software. Please refer to 5.2.3 and 5.2.4 for guidance. The latest version of antivirus installed with the most current virus definitions provides the best protection against viruses.

5.8 Scan your movable/secondary or removable storage devices and hard drive of your personal computers.

6. **Proper use and maintenance of desktop/laptop computers and other ICT equipment**

6.1 Know what processor your computer has, how much random access memory (RAM) is installed, and how big your hard drive is.

6.2 Use the system's built-in utilities. Hard drive stores information by scattering it on the hard drive, and eventually this fragmentation slows down the computer. Run Disk Defragmenter (for Windows) or a similar application periodically to consolidate the data and keep your drive organized. Also, utilities like ScanDisk for Windows can repair disk problems and make your computer more efficient.

6.3 Update the installed an antivirus program, and set it to scan your system every first working day of the week. (Refer to 5.2.3 and 5.2.4) You should also set the application to scan every file you download.

6.4 Back up regularly. Make a habit of backing up all your important files at least once a month or when the need arises.

6.5 To keep your computer running smoothly, it is important to keep the files and folders uncluttered. Cluttered or unorganized folders make it more difficult to find the files you need. Additionally, unwanted files can eventually fill up your hard drive, which will make your computer slower and harder to use. Below are few things you can do to delete unwanted files and improve your computer's performance:

6.5.1 If have any unwanted files, you can delete them manually. To do this, simply drag them into the Recycle Bin (or Trash), and then empty the Recycle Bin.
6.5.2 Windows includes a Disk Defragmenter program in the Control Panel. It scans the files on your hard drive and then rearranges them so that it can read them faster. If your computer is running slowly, running Disk Defragmenter can help to speed it up.
6.5.3 Windows also includes a Disk Cleanup program in the Control Panel. It scans your computer for temporary files and other files that can be deleted. You can then delete the files to free up space on your hard drive.

6.6 Do not delete programs manually. Use either your computer's uninstall utility or a separate uninstall program to remove software you no longer need.

6.7 Shut down your computer properly, and respond to warnings and error messages promptly.

6.8 Clean your computer regularly to keep it working properly and avoid expensive repairs.

6.9 All COA-owned computers and IT equipment bear sticker/label for inventory and monitoring purposes. Removal/destruction of the sticker/ label is strictly prohibited.

7. **Creating a safe work space by avoiding strain and injury**

Using a computer involves a lot of repetitive motions such as typing and using the mouse. Over time, these motions can begin to take their toll on your body, especially your wrists, neck and back. Staring at a monitor for long periods of time can also cause eye strain. To minimize this, you should take a few moments to make sure your workspace is arranged in a comfortable and healthy way.

Here are a few tips to help you avoid injury in your workspace:

7.1 Make sure your chair is adjusted to allow you to sit in a comfortable position. Many office chairs are especially designed to support the lower back and promote good posture.

7.2 Try to place the keyboard in a position that allows you to keep your wrists straight and relaxed, to avoid wrist strain. Many desks have a keyboard tray that may keep the keyboard at a better height.

7.3 Keep the mouse close to the keyboard: If possible, place the mouse right next to the keyboard. If the mouse is too far away, it may be uncomfortable or awkward to reach for the mouse.

7.4 Place the monitor at a comfortable distance: The ideal position for a monitor is 20 to 40 inches away from your eyes. It should also be at eye level or slightly lower.

7.5 Avoid clutter: The computer area can quickly become cluttered with papers, computer accessories, and other items. By keeping this area as uncluttered as possible, you can improve your productivity and also prevent strain or injury.

7.6 Take frequent breaks: It's important to take breaks while working at your computer. To avoid eye strain, you should look away from the monitor every once in a while. You can also stand up and walk around to avoid sitting in the same position for long periods of time.

II. DEFINITION OF TERMS

1. Firewall – can either be software based or hardware based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secured and trusted.

2. Freeware - software that is available for use at no cost but usually with one or more restricted usage rights. (adobe reader, Skype)

3. Internet – the unifying, super network of computer resources that interconnects smaller networks for the purpose of sharing and presenting data. When taken apart from its graphical interface (www, or World Wide Web), the Internet is a text-based information exchange using communication protocols, comprising data repositories accessed with FTP clients, topic-based user groups and forums, and similar forms of digital information exchange.

4. Macro Virus –is a virus that is written in a macro language: that is to say, a language built into a software application such as word processor. Since some applications (notably, but not exclusively, the parts of Microsoft Office) allow macro programs to be embedded in documents, so that the programs may be run automatically when the document is opened, this provides a distinct mechanism by which viruses can be spread.

5. Malware – short of malicious software. Includes all computer viruses, worms, Trojan horses or other, similar programs that have the potential of damaging files stored on the system, affecting the performance of any application, or degrading the overall performance of the Commission's computer network.

6. Offensive Material – material that serves to defame, ridicule, intimidate, or otherwise affront or antagonize other employees.

7. Shareware - is proprietary software that is provided to users without payment on a trial basis and is often limited by any combination of functionality, availability (it may be functional for a limited period only), or convenience (the software may present a dialog at startup or during usage, reminding the user to purchase it). The rationale behind shareware is to give buyers the opportunity to use the program and judge its usefulness before purchasing a license for the full version of the software.

8. Technology resources – consist of computing, networking, and software applications that can be accessed by authorized users.

9. Trojan horse – a type of destructive malware that arrives as part of an e-mail attachment and which otherwise appears harmless; however, it can affect the operation of the computer on which it is activated. Trojan horses do not typically infect other computers or spread from one computer to another.

10. User – anyone with authorized access to the Commission's technology resources including permanent and temporary employees or third party personnel such as contractors, consultants.

11. Virus and e-mail virus – pieces of code that "piggyback" on other programs and files that are transferred between computers by way of downloads, e-mail, or other types of file transfers. Each time the program is run, the file is activated, and can replicate itself and create havoc on the network by using up computer resources. E-mail viruses often replicate themselves automatically, and can infect an e-mail address book, sending itself out to dozens or even hundreds of other e-mail users.

12. World wide web – the Internet's graphical interface, accessed by way of Web browsers such as MS Internet Explorer, Netscape Navigator, Safari, Mozilla, etc., which enable users to view hyperlinked, HTML-formatted Web "pages" that can contain all manner of products, information, and other visual or text-based content

III. ITO HELP DESK

Any concerns/clarifications on these guidelines please feel free to contact the ITO Administrator/Help Desk at local 4018 or e-mail us at coaweb@coa.gov.ph.

IV. ENFORCEMENT

Any user found to have violated any of the guidelines may be denied access to the ICT resources and may be subjected to disciplinary action.

Breaches of these guidelines by a third party may lead to the withdrawal of privileges and access granted to the Commission's ICT resources.

V. UPDATE AND NOTIFICATION

These guidelines are expected to evolve through updates and continuous effort shall be made to keep abreast with the ever changing technology and to maintain its relevance and acceptability. Updates shall be issued as they are developed.

Annex A

USER ACCESS REQUEST FORM

ITO Form No. 01

NAME	DATE
REQUESTING SECTION/DIVISION/OFFICE	**TELEPHONE NUMBER/LOCAL**

ACCESS REQUESTED

☐ Internet

☐ E-Mail (MS Outlook Account)

Application

☐ PMIS ☐ ALEMS ☐ BIOMETRICS ☐ OTHERS

Please Specify

PURPOSE	For MS Outlook Account I am aware that if I will not open my Outlook account for three consecutive months said account will be deleted. _____ Signature
APPROVED _____ Director/Authorized Signatory	**CONFIDENTIALITY CLAUSE** I hereby acknowledge acceptance of a user ID and password, which allows the undersigned to access the Commission's ICT resources. I understand that my User ID and Password are to be kept confidential and I must only access the information in which I have direct and legitimate use in the performance of my duties and functions. I agree to follow all procedures designed to protect confidential information. _____ Signature

UARF Ver 1.0