



USAID
FROM THE AMERICAN PEOPLE



EISA DEPARTMENTAL POLICY – COMPUTING AND COMMUNICATIONS ACCEPTABLE USE POLICY

12/10/2006

This publication was produced for review by the United States Agency for International Development. It was prepared by BearingPoint, Inc.

EISA DEPARTMENTAL POLICY

COMPUTING AND COMMUNICATIONS ACCEPTABLE USE POLICY

TECHNICAL ASSISTANCE FOR POLICY REFORM II

CONTRACT NUMBER: 263-C-00-05-00063-00

BEARINGPOINT, INC.

USAID/EGYPT POLICY AND PRIVATE SECTOR OFFICE

DISCLAIMER:

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

Policy

EISA encourages its officers and employees to enhance customer services, productivity and increase knowledge through the use of available computing and electronic communications facilities, including the use of the Internet, within the bounds of their employment, and legal and ethical conduct requirements.

The policy is intended to cover EISA staff use of the following facilities:

- All computer hardware, network and communications equipment
- All computer software and applications, including all Internet applications
- Telephones and fax machines

Guidelines

Use of any EISA computing or communication resources by an officer or employee should be restricted to employment related purposes. Employees are strictly prohibited from using the computing or communication resources for immoral or illegal activities.

Common sense should dictate what is and is not employment related, and also what constitutes illegal and unethical behaviour in this regard. The following are specifically prohibited:

- Private commercial activities for the purpose of personal gain.
- Accessing, distributing or disclosing material prohibited by policy or law
- Breaching confidentiality.
- Unauthorised copy or transmission of copyrighted material
- Transmitting threatening, abusive, defamatory or offensive material
- Distributing chain letters.
- False representation.
- Unauthorised use or release of Department information.
- Unauthorised access to and use of computers.

Responsibilities

When using government computing and communications resources and facilities, officers are expected to be aware of their responsibilities to:

- Comply with all legal, legislative and administrative requirements.

- Ensure any action taken serves to enhance the services provided by the Department, and not bring the Department into disrepute.
- Be informed of all security requirements related to the use of computer facilities, and in particular the security risks involved in using the Internet and ensure that this is not compromised by their actions.
- Seek advice if they are unsure about the status of their actions.

Officers and Employees who knowingly breach this policy will be dealt with under the disciplinary provisions of EISA.

While it is the individual officer's or employee's responsibility to use resources appropriately, management also has a responsibility to deal with both deliberate and inadvertent breaches of the policy.

Storage of Information and Monitoring of Use

Staff are advised that all information, stored on the EISA Network Servers is backed up nightly. Similarly detailed statistics on usage of the telephone systems and the Internet are automatically logged and records kept on backup tapes.

Monthly backup tapes are kept for several years.

Systems are backed up primarily for disaster recovery purposes. However, legitimate requests for this information may be scrutinized or made public.

Systems are also routinely monitored by IT staff to ensure satisfactory levels of service. Monitoring may also be carried out at the instruction of the Chairman. Instances of blatant abuse of this policy will be reported to the Chairman.

Passwords

The use of your computer, email and the Internet is monitored through a "user id" and access rights governed by a password personal to you. Do not divulge your password to others because you could be held responsible for their actions. Do not login as another user. Store a copy of your password in a secure location (never attach it to your monitor). You may be required to divulge your password to an EISA manager or IT staff person. This is acceptable, but you should change your password at a convenient opportunity after you have divulged your password.

Email Specific Procedures

1. Sending and Receiving Email

- a) Sending email to broadcast groups (e.g. *All EISA employees*) is to be used with discretion. Email sent to all EISA employees or large industry groups must be approved by the appropriate manager prior to being sent.
- b) Email sent to multiple external recipients (e.g. Newsletters) must be addressed using the Bcc (Blind Copy) address block. unless the distribution list is below 10 addresses and or the privacy of recipients is not a consideration (e.g. members of a working group)
- c) All email messages sent through the departmental system contain a standard disclaimer/legal notice. This disclaimer will be provided by EISA.
- d) If staff are sending a confidential message, it is necessary to mark the item as such.
- e) If the item is not for further distribution (other than the intended recipient) and is subject to copyright considerations, it is the responsibility of the sender to clearly indicate this in the email.
- f) Emails related to the EISA's business activities are critical records and must be captured in the records system.
- g) Officers and Employees of EISA may maintain a personal email account for personal use such as (hotmail, gmail etc.). These accounts should never be used for business related purposes. In addition, these emails should never be stored on the EISA workstation or server computers.
- h) EISA will store all emails on the Exchange server. An employee may at their own discretion save email to their local workstation.
- i) It is the responsibility of all EISA staff to limit the mail stored in their email account. Therefore, email which is of a trivial nature should be deleted after a reasonable retention period. Emails of a critical business nature may be stored permanently.
- j) Employees should create meaningful sub folders for their email. The inbox folder should be kept to a limited number of recent emails waiting to be moved to appropriate sub folders.
- k) Email attachments (either sending or receiving) should be limited to 10 megabytes in size. If an attachment needs to exceed this size please

contact the IT department for approval and possible alternative method of sending or receiving.

2. Email Formats

Recommended format for electronic mail communications is:

- a) Messages should be transmitted as 'text' or 'rich text'.
- b) Messages should not be transmitted as 'html'.
- c) Messages should not contain additional graphic images that are not essential to the purpose of the message.
- d) Messages should use fonts that are easy to read on the screen.”

3. SPAM Email

The following procedures should be employed to address and prevent SPAM emails.

- a) Report any excessive SPAM receipt to the IT department.
- b) Do not respond to solicitations with your EISA email address.
- c) SPAM filters should only be employed under the direction of the IT department.
- d) Avoid opening any mail that is suspected of being SPAM.
- e) Sending of SPAM is prohibited from any EISA email.

4. Arrangements for Leave

Given that people use email with the expectation of receiving a timely response, arrangements should be made for email when a staff member takes leave.

Staff taking leave must ensure that, in their absence, their mail-boxes are set up to:

- a) Ensure that all incoming emails are considered during their leave.
- b) Provide automated replies to senders advising of their absence and providing email, fax and telephone contact details of the person undertaking duties while they are away. Consult the IT department for technical assistance in this area.
- c) Remove themselves if possible from broadcast groups or list servers prior to taking leave.
- d) Staff taking leave should consider allowing proxy email access to another staff member. Automated replies should be removed as soon as staff resume their duties”.

Internet Usage

Subscription to list servers is to be kept to those that relate to the agency's activities - subscription to lists that are not work related is not permitted.

EISA will monitor usage of the Internet by employees, including reviewing a list of web sites accessed by an individual. No individual should have any expectation of privacy in terms of their usage of the Internet. In addition, EISA will restrict access to certain sites that it deems are not necessary for work related purposes. These include sites that contain illegal, obscene, pornographic or hateful content, which is objectionable or inappropriate in the workplace. Even if a site is attainable through the EISA network do not consider it an acceptable site. It is the responsibility of the employee to avoid unacceptable sites.

Software may not be downloaded from the Internet without prior approval of the IT Department. In addition, anti-virus download software is not to be disabled. All computers are configured to automatically scan any material downloaded from the Internet.

The Internet provides access to many sites that charge a subscription or usage fee to access and use the information on the site. If costs are appropriately incurred on behalf of the EISA, the user may submit the charges for reimbursement on expense reports, subject to customary review by the EISA management. All items that are charged to the EISA are subject to the same approval process as other business-related expenses. Requests for approval should be submitted to the appropriate manager.

Unacceptable Use of Internet

The following activities are prohibited from any EISA workstation or laptop computer.

1. Use of the Internet for any purpose that violates Egyptian law or any Code or Policies, Standards and Procedures.
2. Use for any for-profit activities.
3. Use for purposes not directly related to the mission, charter, or work tasks of the EISA.
4. Use for private business, including commercial advertising.
5. Use for access to and distribution of:

- a) Indecent or obscene material.
 - b) Pornography.
6. Downloading, Use of, or and distribution of computer games, music, videos, or images that have no bearing on the EISA's mission is prohibited.
 7. Use that interferes with, or disrupts, network users, services, or equipment.
 8. Use of Internet services to seek out information, distribute information, obtain copies of, or modify files and other data, which is private, confidential, or not open to public inspection, or release such information unless specifically authorised to do so once the legal conditions for release are satisfied.
 9. No intentional copy is to be made of any software, electronic file, program, or data without a prior, good faith determination that such copying is, in fact, permissible. Any efforts to obtain permission should be adequately documented.
 10. Users shall not misrepresent themselves as other persons on the Internet, without the expressed consent of those other persons. Users shall not circumvent established policies defining eligibility for access to information or systems.
 11. Use of Internet Services to develop programs designed to harass other users, or infiltrate a computer or computing system, and/or damage or alter the software components of systems. Examples are viruses and Trojan horse programs.
 12. Use for fundraising or public relations activities not specifically related to EISA's activities.

Computer Equipment Usage

Computer equipment is to remain at EISA offices at all times unless approval from the IT department and the appropriate manager has been received in advance. This includes all types of computer equipment including laptops, desktops, removable disk drives, flash drives, monitors, mouse, keyboards etc.

Any equipment removed from EISA with permission must be appropriately signed for stating the name of user, date and time of removal, expected date of return, and purpose for removal.

Technical Assistance for Policy Reform II
BearingPoint, Inc,
18 El Sad El Aali Street, 18th Floor,
Dokki, Giza
Egypt
Country Code: 12311
Phone: +2 02 335 5507
Fax: +2 02 337 7684
Web address: www.usaideconomic.org.eg