Division of Accounting – Policies and Procedures Manual Standard Policies and Procedures	
Policy Number-AUB-05-01	**Revision Number: 4**
Subject: **Electronic Communication Appropriate Use**	**Effective Date: 10-01-2009**
	Superintendent Approval:
	General Manager Approval:

1.0 PURPOSE

Athens Utilities Board (AUB) recognizes the increase in technology resources available to employees designed to enable AUB to provide service in a more timely and efficient manner. Employees and contractors are expected to use any utility-owned electronic communications devices in a manner consistent with this policy.

2.0 SCOPE

This policy applies to any and all use of electronic communication equipment by employees or approved contractors. Electronic communication devices include, but are not limited to, radios, telephones, cellular phones, faxes, all computer systems and peripherals, e-mail systems, internet and network resources.

3.0 ACCESS AND OWNERSHIP OF INFORMATION

Electronic communications devices are provided to increase the efficiency with which AUB serves its customers. All information processed through or by any electronic communication device owned by AUB will be the property of AUB. All such information shall be subject to inspection at any time. AUB reserves the right to inspect any electronic communication or related device with no advance notice. Also, all electronic information will be made available to the Network Administrator in the event of absence, transfer, vacation or termination.

4.0 MONITORING

AUB reserves to right to monitor electronic communications of its employees. E-mail may be a public record that is subject to public inspection. AUB shall comply with all federal laws relative to monitoring electronic communications.

5.0 PERSONAL USE

Under no circumstances should AUB electronic communication equipment be used for political purposes or for employment outside AUB. Persons who are not employees of AUB, or approved contractors, should be permitted to use the utility's electronic communications equipment only in case of an emergency. Employees will reimburse AUB for any cost incurred for personal use of any electronic communication equipment.

6.0 INAPPROPRIATE USES

Legal precedence has been established whereby employers may be held liable for their employees' inappropriate use of electronic communication devices. AUB will consider any inappropriate use of electronic communication equipment and systems as a serious offense. Inappropriate uses of electronic communication equipment include, but are not limited to:

- Activity violating AUB policy;
- Any use relative to outside employment, or using any AUB resources for personal gain;
- Disclosure of confidential information;
- Use for any political purposes;
- Use to store, transmit, load, view or download sexually explicit material and images, violent images and material, or any other material or language that may be offensive to others;
- Any use of harassing, intimidating, discriminating, or threatening language;
- Violations of federal copyright laws or software licensing agreements;
- Playing or installing any computer games;
- Activity violating any federal, state or local laws;
- Stealing, using, or disclosing someone else's user ID or password without authorization;
- Sending or posting messages that defame or slander other individuals;
- Refusing to cooperate with any security investigation;
- Political causes or activities, religious activities, or any type of gambling;
- Communicating personal views as representing those of the organization;
- Sending anonymous e-mail messages;

7.0 E-MAIL AND INTERNET

E-mail and internet access are provided to improve productivity. These tools should be used predominantly for company business. Under no circumstance should any use of E-Mail or Internet, other than appropriate business use, result in any additional cost to AUB. Superintendents shall have the responsibility of determining which employees in their respective divisions will have E-Mail and Internet access. This decision will be based on business need only. Superintendents will advise the Network Administrator of all additions and deletions of access to these tools.

AUB reserves the right to monitor all e-mail and internet activity processed through its equipment. Any information processed through, or stored on, any of AUB's computer equipment is the property of AUB. Information transmitted via e-mail is not secure. Because of this fact, employees are prohibited from transferring any confidential information via e-mail.

8.0 PERSONAL COMPUTERS AND DATA SECURITY

Because of the sensitive nature of certain systems within AUB, passwords may be assigned. Passwords are designed to protect systems from unauthorized access. Employees should not use such obvious passwords as a child's or spouse's name. Passwords should be a word or phrase that is not readily determinable. Employees should never share their password with other personnel, or record them in written form. Passwords should be committed to memory. Passwords should never be posted on a computer terminal, under the keyboard, or anywhere accessible to unauthorized users.

No software will be installed on any of the utility's computer equipment without the prior approval of the Network Administrator. Under no circumstances will pirated software be installed on any AUB computer equipment. Any software installed on AUB computers should be properly licensed to AUB. It is a violation of this policy to install any software that is licensed to anyone other than the utility on any AUB equipment. No files should be downloaded from the internet, or copied from any storage medium, without prior approval from the Network Administrator. It will be the responsibility of the Network Administrator to ensure that all virus protection software is updated at an appropriate frequency. All systems will be properly protected by virus detection software. In the event of a serious virus threat, the Network Administrator will have the authority to disable any systems.

Employees should not alter the hardware configuration of any systems. All hardware changes should be performed by the Network Administrator, or his/her designee. No components will be added to, or taken from, any systems without permission from the Network Administrator. Employees should exercise caution with food and drink around any electronic equipment. Persons who are not under the employ of AUB or contracted to provide service to AUB will not be permitted access to any AUB computer systems.

The viewing, altering, transmitting, accessing, copying, or deleting of files belonging to another employee without their prior consent is prohibited. However, the Network Administrator may delete certain files while performing regular maintenance procedures. Each individual user will be responsible for backing up data stored on the local drives of their respective systems. The Network Administrator will be responsible for backing up all data written to network systems. Copies of network backups will be stored offsite. These backup copies will be rotated at a regular frequency.