Leon County Research and Development Authority

Policy No. 11-10

Title: Internet Security and E-mail Policy

Date Adopted: August 2, 2011

Effective Date: August 2, 2011

---

1. PURPOSE

The purpose of Policy No. 11-10, "Internet Security and E-mail Policy" is to provide the policies and procedures with respect to E-mail and Internet usage that protects the integrity of the data entrusted to the Board of Governors and employees of the Leon County Research and Development Authority (hereinafter referred to as the "Authority").

2. SCOPE

This Policy is designed to protect the Authority, its employees, and its resources from the risks associated with usage of the Internet and the worldwide web. To ensure that resources are available for work related purposes, the goals of this Policy are to outline appropriate and inappropriate use of Authority Internet and Computer resources, including the use of browsers, electronic mail (e-mail), instant messaging, social media/networking, file uploads and downloads, and voice communication. The provisions of this Policy are applicable to the Authority's Board of Governors, employees, and all users of the Authority's internet and computer resources.

3. DEFINITIONS

As used in this Policy, the following terms shall have the following meanings:

a. "Authority's Computer System" means the Authority's wired and wireless networks, servers, and end-user devices; including, but not limited to, desktops, laptops, smart phones, and other wired or wireless devices.

b. "Social Media/Networking" means internet-based technologies that enable individuals to communicate through the sharing of content, interacting, and collaborating through bi-

directional applications or messaging, and developing communities around common interests.

c. "User" means any Board member, employee, or visitor to the Authority.

4. GUIDELINES

a. Computer Security The following procedures relating to computer security shall be followed for all computers, which contain Authority information, in order to protect the integrity of the data entrusted to the officers and employees of the Authority:

   i. All users shall use the screen saver password function supplied with the computer operating system.

   ii. All users shall change passwords every 90 days.

   iii. All passwords used shall conform to the following standards:

      1. contain no less than six characters
      2. contain at least one non-alpha character
      3. contain at least one numeric digit
      4. contain no more than two letters, in sequence, of the user-name
      5. contain no more than two letters, in sequence, of the reversed user-name

   iv. Passwords shall not be written down, communicated to others or shared among employees.

   v. Electronic data, or applications, brought to the Authority from another location shall be checked for computer virus infections prior to connecting to the Authority's network.

b. Prohibited Uses

Neither the Authority's Computer System nor e-mail or Internet access systems shall be used in any of the following ways:

   i. To harass, intimidate, or threaten another person. Users should not transmit to others or display images, sounds, or messages that might be perceived by a reasonable person as being, or have been identified as, harassing.

   ii. To access or distribute obscene, abusive, libelous, or defamatory material

   iii. To reproduce or distribute copyrighted materials which are not authorized for reproduction or distribution

iv. To copy or use software, except as explicitly permitted under licensing agreements. Users should be able to prove ownership of software in their possession.

v. To impersonate another user or mislead a recipient about one's identity

vi. To access another person's e-mail, or Social Media/Networking account/address, if not specifically authorized to do so

vii. To bypass the Authority's Computer Systems' security mechanisms or undermine the security or the integrity of computing systems or networks or to attempt to gain unauthorized access. Users may not use any computer program or device to intercept or decode passwords or similar access control information. Security gaps should be reported to Authority staff.

viii. To send or create junk mail, spams, chain letters, computer viruses or hoaxes, or other disruptive material.

ix. To communicate the Authority's official position on any matter, unless specifically authorized to make such statements on behalf of the Authority

x. For any purpose which is illegal, against Authority policy, or contrary to the Authority's best interests.

xi. To pursue an individual's private business interests which are unrelated to the Authority

xii. To conduct any type of non-Authority approved solicitation

xiii. To delete or destroy public records without authorization.

b. <u>Permissible Uses</u>

E-mail and the Internet are to be used primarily to facilitate Authority business. However, not all personal use of e-mail and the Internet is forbidden. Reasonable personal use is permitted consistent with the provisions of this Section. Non-Authority business related e-mail and Internet usage is permitted, provided such use is brief, does not interfere with work, does not subject the Authority to any additional costs, and is otherwise consistent with requirements set forth in this Policy. With prior permission of his or her supervisor, an employee is permitted to briefly visit non-inappropriate Internet sites during non-work time; such as, break, lunch, and before or after work hours.

c. Privacy

No guarantee can be made for the privacy of any communication on the network. Computer passwords are for security purposes only and are no guarantee of the privacy or confidentiality of any user's utilization of the Authority's Computer System. The Authority's Executive Director will have administrative rights access to the Authority's Computer System.

d. Logged and Blocked Access to Non-Work Related Internet Usage

As a result of potential negative impact to network services, the Authority shall have the discretionary authority, to audit, inspect, and/or log network resource utilization and block non work-related Internet access, consistent with this section.

i. Logged and Blocked Access

The Authority maintains the right to utilize software that makes it possible to identify and/or block access to Internet sites containing sexually explicit or other material deemed inappropriate for the workplace, and log any and all aspects of the Authority's Computer System and network. Users who must access blocked sites for work related purposes shall get written approval from the Executive Director.

e. Violation of Policy

i. Users of the Authority Computer System found to be in violation of this Policy may no longer be permitted use of the System and may be subject to civil and criminal liability.

ii. Any employee found to be in violation of any provision of this Policy shall be subject to disciplinary action up to and including dismissal, civil and criminal liability. The Authority may refer suspected violations of applicable law to appropriate law enforcement agencies.

f. Communication of the Policy to Employees and Users of the System

The Executive Director of the Authority will be responsible for communicating this Policy to all Board members, employees and users of the Authority's Computer System.