Policy: Information Security

Issuing Dept: Information Technology

Effective Date: 11-17-09

Approved By:

Linda Watson
Chief Executive Officer

SCOPE

This policy applies to ALL Authority Employees.

POLICY

Introduction

The Authority is committed to providing an environment that encourages the use of computers and electronic information. It is the responsibility of each employee to ensure that this technology is used for proper business purposes and in a manner that does not compromise the confidentiality of proprietary or other sensitive information. This policy covers all uses of Authority electronic communications and computer systems. Violations of this policy will subject the employee to disciplinary measures up to and including dismissal.

This policy covers procedures on the following:

- Computer hardware and software
- Email
- Internet access

COMPUTER HARDWARE AND SOFTWARE

Ownership

All computer system networks, computer equipment, Point Of Sale systems, other electronic communications systems, and all communications and stored information transmitted, received or contained in Authority information systems are the Authority's property and are to be used for business related purposes. Any personal use of such systems should be incidental and limited to avoid unnecessary interference with your business responsibilities and unnecessary burden on any of the Authority's electronic communications systems.

Avoiding Viruses

To limit the Authority's exposure to computer viruses, avoid software conflicts and software license violations, and to properly manage our information systems, only the Information Technology (IT) Division may install software onto any Authority computer. Unauthorized software installed onto any Authority computer will be immediately removed. Unauthorized software includes but is not limited to personal programs such as screen savers, games, browser add-ins (Yahoo, weather bug), etc.

Troubleshooting

All Authority computer software or hardware problems and questions should be directed to the IT Division. For certain systems and applications, external help desks are provided for better service and coverage. These help desks should be used first to resolve issues faster and more efficiently.

Virus Alert

All Authority email and programs are scanned for viruses as they enter our network. If a virus is found, the appropriate action is taken by the anti-virus software. If you receive notification that a virus has been found on your computer, contact the IT Division immediately. All Authority computers have been configured with anti-virus software and it should not be disabled for any reason at any time.

Access Codes and Passwords

The confidentiality and integrity of data stored on the Authority's computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties

E-MAIL POLICIES AND PROCEDURES

Business Purpose Only

The Authority email system is for business purposes. Any personal use of such systems should be incidental and limited to avoid unnecessary interference with your business responsibilities and unnecessary burden on any of the Authority's electronic communications systems.

No Expectation of Privacy

Nothing that is transmitted via Authority email is confidential or private despite any such designation either by the sender or the recipient. Security passwords that are issued to employees are for the purpose of protecting the security of the Authority, not for any individual's interests in privacy. The Authority reserves the right to monitor its email system including an employee's mailbox at any time at its sole discretion in accordance with applicable law.

Certain Messages Prohibited

Employees are strictly prohibited from viewing, sending, saving or printing email messages that may be viewed as inappropriate or offensive including but not limited to messages containing obscene, vulgar, or 'off color' language; messages that may be discriminatory or harassing to other employees including but not limited to harassment of any type (sex, race, age, etc.); messages that may hold persons up to ridicule or disparagement, false statements or name calling; and use of sarcasm.

Limited Distribution

Email messages should be distributed only to those individuals who have a business need to receive them.

INTERNET ACCESS POLICIES AND PROCEDURES

Application of Internal Email Policies and Procedures

Authority policies and procedures concerning email above also apply to Internet access.

Unauthorized Use of the Internet

Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes but is not limited to connecting, posting, or downloading pornographic, inappropriate, or obscene material; engaging in computer "hacking" and other related activities; or attempting to disable or compromise the security of information contained on Authority computers (or otherwise using Authority computers for personal use).

Confidentiality

Internet messages should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way, even if the messages are encrypted.

Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature be placed on the Internet. Because information placed on the Internet may display the Authority's address, the accuracy of the information must reflect the standards and policies of the Authority.

Downloading from the Internet is Prohibited

Downloading software or any executable files from the Internet is prohibited (e.g., games, applications).