517 Information Technology Use

Effective Date: 4/1/2010 *Revision Date:*

The Authority owns and operates various computer systems, which are provided for use by employees to perform their jobs. All users are responsible for seeing that these facilities are used in an effective, ethical, and lawful manner. The procedures and principles presented in this policy apply to all Authority employees, elected officials, volunteers and other affiliates who use Authority-provided computer systems, regardless of the user's location when accessing the network. For purposes of this policy, the term "employee" includes all of the preceding categories.

This policy sets forth generally applicable policies that apply when employees use the information systems and equipment provided by the Authority. Violations of this policy are subject to discipline, up to and including termination. Persons who use Authority systems or equipment for defamatory, illegal, or fraudulent purposes, or who break into unauthorized areas of the Authority's systems, may also be subject to civil liability and criminal prosecution.

Use of Authority Equipment

All Authority property, including computers, e-mail, voicemail, internet service, telephone systems, fax machines, wire services, and other equipment and services, is provided for business use. Limited, occasional use of these Authority systems for personal, non-business purposes is permitted. Employees must demonstrate good judgment in this use. Personal use of Authority systems must be limited to non-working time, and must not be disruptive to the work of any employee. Also, use of Authority systems for promoting, buying or selling goods or services, or group solicitations, is prohibited, since these types of activities are limited to posting on the bulletin boards specifically designated for this purpose. Equipment may not be modified in any way except by authorized personnel.

Security

All users of Authority systems are required to maintain the security and integrity of Authority systems and information from access by unauthorized persons. Workspaces and equipment must not be left unattended in a manner that could permit any unauthorized person to obtain unauthorized access. Authorized use must be only with the user's own log-in, password, or other access device. Users may not share log-ins, passwords, or access devices with any other person, except when business needs require and an appropriate manager has given written authorization.

Authority Access and Monitoring

Employees should not assume that electronic communications are private. Security procedures, such as passwords, are designed to control access to Authority systems, not to guarantee the personal privacy or confidentiality of any message or document. Employees should keep personal records and information at home, as the Authority does not provide privacy or confidentiality of non-business information stored in files (electronic or hard copy) at work.

The Authority reserves the right to access and review everything on all information systems and equipment, including directories, diskettes, files, data bases, e-mail messages, voicemail messages and any data stored or used in connection with Authority information systems. Electronic files that have been deleted or erased may remain stored in the Authority's computer or telephone systems. The Authority retains the right to access such information for as long as it may be obtained from any source, even after it has been deleted or erased. All e-mail messages are archived and stored on an Authority server pursuant to the Authority's retention policies.

The Authority monitors individual use patterns (telephone numbers dialed, web sites accessed, call lengths, etc.) to evaluate the optimum utilization of technology resources, and to detect patterns of use that could suggest improper or illegal activity. The Authority may employ web filtering and block websites based on categories determined by the Authority.

Each employee who uses Authority communication systems, by doing so, consents to the Authority monitoring his or her communications over those systems, as authorized by law, when the Authority finds that a business reason warrants it.

E-mail Communications and Internet Use

The Authority strictly prohibits the use of information and communication systems for any communication or activity which is obscene, pornographic, profane, abusive, defamatory, derogatory, discriminatory, a violation of any civil or criminal law or statute, or a violation of any Authority policy or standard. If a user has any question about whether a particular use or communication is improper, it is the user's responsibility to ask an appropriate supervisor before engaging in the activity.

Revealing Authority business information, employee or customer by e-mail or the internet is prohibited. Any other messages that may adversely affect the Authority, its customers, the public or employees are also prohibited. Internet and e-mail may not be used for personal gain, personal business, or advancement of personal views. No one should make any on-line statement about the Authority except as expressly authorized by senior management. If you have any question about whether a particular use is improper, ask an appropriate supervisor before engaging in the activity.

Communicating anonymously or by an assumed name is prohibited. E-mail messages should be written in a professional manner. Consider your routing list carefully and exercise the same care you would with any written document before sending an electronic message.

Delete or archive unwanted and obsolete messages. It is each employee's responsibility to keep their mailboxes manageable and up to date. All messages are archived automatically.

If you receive an e-mail message from an unknown sender, delete the message to prevent viruses and other risks to Authority information systems. If you receive a message that was not intended for you, inform the sender immediately and delete the message from your mailbox.

Users of Authority equipment may not access any external or public computer or network, except for specific business purposes with express authorization by a supervisor. Any user who is authorized to connect to any outside computer or network is obligated to take all necessary measures to ensure the security of the Authority's systems and information. Employees may not install, add, or download any other computer software to Authority systems without prior approval by the Authority.

Employees may not:

- Monitor or intercept anything on the Authority's computer system without authorization
- Obtain unauthorized access to any part of the Authority's information system
- Use Authority systems to obtain unauthorized access to any other computer or system
- Use anyone else's log-ins or passwords without Authority permission
- Use Authority systems in a way that has the purpose or effect of concealing or disguising the user's identity

Software

The Authority has acquired rights to use certain software programs on the Authority's communication and information systems for business purposes. Software is protected by copyright law. The Authority's right to use software is subject to license agreements with the publisher or seller of the software. Those license agreements generally prohibit users from copying, selling, loaning, or giving away software, or using or duplicating it in any way that is not expressly authorized by the license agreement. Therefore, any software that is available through the Authority's information systems may not be used in any way other than in the regular course of Authority business.

Only Information Systems personnel or agents contracted by them may install or remove software or hardware on any Authority computer system. Information Systems personnel may, at their discretion, authorize staff to perform specific software or hardware installations. All other software or hardware installations are strictly prohibited.

Portable Devices

The Authority may provide employees with portable technology, including laptop computers, cell phones, and personal digital assistants (PDAs), in order to support Authority business. Such portable technology is to be used solely by the employee and solely for the benefit of the Authority. Upon termination of employment, or upon request by the Authority, each employee must immediately return to the Authority all equipment which is Authority property or contains any confidential or proprietary information belonging to the Authority or its clients/customers or the public. Employees are strictly prohibited from using any portable technology for Authority business unless the portable technology is owned and provided by the Authority. Use of non-Authority-owned laptop computers, cell phones, PDAs, or other portable technology for Authority business, including the access, sharing, or retrieval of information from Authority systems, is not permitted.

Telecommuting

Any employee working from home or telecommuting to any significant degree will be required to sign an agreement stating the terms under which he or she will be permitted to telecommute, and creating reasonable protections for the use and transmittal of Authority information.

Publishing to the Internet

Only Information Systems Personnel and assigned Authority personnel should publish to the Internet. This ensures that the information being released about the Authority is appropriate and projects a positive image of the Authority.