Employee Computer Use Policy

WIFA Policy #: IV.1

Purpose:

To define WIFA employee computer use policy and standards.

Policy:

Section 1: Policy Scope

This policy applies to the general use of all WIFA computers.

Section 2: Definitions

For purposes of this policy, the following definitions shall apply:

a. "*Electronic communications*" shall mean and include the use of information systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, World Wide Web (internet), or other such electronic tools.

b. "*Information systems*" shall mean and include computers, networks, servers and other similar devices that are administered by WIFA and for which WIFA is responsible.

c. "*Networks*" shall mean and include video, voice and data networks, routers and storage devices.

c. "*Obscene*" with respect to obscene material shall mean:

(1) That an average person applying contemporary community standards would find the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion.

(2) The material depicts or describes in a patently offensive way sexual conduct specifically set out in ARS Title 13, Chapter 35

d. "*Virus*" A program or code that replicates, that is, infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium.

e. "*Worm*" A program that makes copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.

Section 3: Computer Use Policy

- **Permitted Use:** Information systems are to be used for WIFA-related business. However, personal use is permitted so long as it conforms to this Policy and does not interfere with the WIFA operations or an employee user's performance of duties, as limited personal use of information systems does not ordinarily result in additional costs to WIFA and may actually result in increased efficiencies. Personal use of any WIFA information system to access, download, print, store, forward, transmit or distribute obscene material is prohibited. **Under all circumstances, personal use by employees must comply with the WIFA policy, state policy, and shall not conflict with an employee's performance of duties and responsibilities for WIFA.**

- **Access:** Unauthorized access to information systems is prohibited. No employee shall use or exchange the ID or password of another; nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate computer maintenance and repairs. When any user terminates his or her relation with WIFA, his or her ID and password shall be denied further access to the WIFA computing resources.

- **User Privacy**: A user can expect the files and data he or she generates to be public information and users should be continuously aware of this fact. As a condition of employment granting Network and Internet access, WIFA has the right to monitor, log and archive all network activity, content and electronic communication, whether related to WIFA business or personal information in nature, including e-mail, temporary internet files, or cache files. **All electronic communications, business or personal, are subject to review by two staff members, one of which is the Executive Director or delegate, and the Information Technology staff at any time, and understand that such information is backed-up, stored and may be accessible even after employee has attempted to delete the information.** Employees have no expectation of privacy in these electronic communications, and understand that monthly Internet usage reports can be furnished to the Executive Director and/or managers. These reports include a list of sites visited by each user and the length of time spent at these sites. Staff understand and agree that if monitoring, logging and archiving of State business or personal electronic communications discloses any activity that is contrary to Internet Use Policy, or any other state policy, administrative rule, or state or federal statute, the information obtained may be used in disciplinary action against the employee, and may be furnished to law enforcement agencies for criminal prosecution.

- **Repair and Maintenance of Equipment**: Users should be aware that duly authorized Information Technology personnel have authority to access individual user files or data in the process of performing repair or maintenance of computing equipment as deemed reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance for WIFA needs. Information Technology personnel performing repair or maintenance of computing equipment are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

- **Response to Misuse of Computers and Network Systems:** When for reasonable cause, as determined by the Executive Director and Information Technology staff, it is believed that an act of misuse as defined in the above sections has occurred, the Executive Director and IT Network Administrator may access any account, file or other data controlled by the alleged violator and share such account information, file or other data with those persons authorized to investigate and implement sanctions associated with the misuse of WIFA computer and information systems. Should the IT Network Administrator reasonably believe that a misuse is present or imminent, such that the potential for damage to the system or the information stored within it, is genuine and serious (e.g. hacking, web chat rooms, instant messaging, spamming or theft), then the IT

Network Administrator, using reasonable belief may take such action as is necessary to protect the information system and the information stored in it, including the denial of access to any WIFA user, without a determination from the Executive Director; provided, however, that the IT Network Administrator shall contact the Executive Director as soon as possible to confirm that any protective actions taken were appropriate and within the parameters of this Policy.

- **All Policies Stated above are Applicable to E-mail**. E-mail should reflect careful, professional and courteous drafting, particularly since it is easily forwarded to others. Copyright laws and license agreements also apply to e-mail. E-mail messages should be deleted once the information contained in them is no longer useful.

Responsibility: Executive Director and IT Network Administrator

Statutory Reference: A.R.S. Title 49, Chapter 8

Rule Reference: N/A

Original Issue Date: February 25, 2004

Previous Amendment Date(s): August 17, 2011

Most Recent Amendment Date: October 6, 2017 (*Replaces All Previous Versions*)

Approval:

Executive Director

10/6/17

Date