EMPLOYEE MANUAL	
Title: **USE OF OFFICE TECHNOLOGY**	
Policy No.: 39.0	Section Nos.: 39.0 – 39.10
Approval Date: February 2021	Effective Date: February 2021
Approved By: Board of Directors	

USE OF OFFICE TECHNOLOGY

The Agency maintains various forms of electronic systems and social media networks to assist in the conduct of the business within the Agency. These systems or networks, including the equipment and the data stored in the systems or networks, are, and remain at all times, the property of the Agency. All messages created, sent, received, or stored in the systems or networks are property of the Agency, and as such may be monitored, recorded, and/or reviewed for quality control and appropriateness of purpose at any time.

The Agency reserves the right to retrieve and review any messages composed, sent or received. Please note that even when a message is deleted or erased, it is still possible to re-create the message. The Agency therefore cannot ensure privacy of any messages to any employee. While voicemail and electronic mail may accommodate the use of passwords for security, confidentiality cannot be guaranteed, and employees are hereby notified that someone other than the intended recipient may review all messages. All passwords must be made known to the Agency in order that all systems or networks are accessible to the Agency when employees are absent.

39.1 Information Technology Requests for Service

Requests for IT service, including the purchase of software and hardware, are to be made using the IT Service Request Link.

39.1.1 Care of Computer Equipment

The primary user of a computer workstation is considered a custodian for the equipment. If the equipment is damaged, lost, stolen, borrowed or is otherwise unavailable for normal business activities, the user must promptly inform the Information Technology Department (IT Department). Computer equipment must not be moved or relocated without the knowledge and approval of the IT Department.

39.1.2 Eating and Drinking

Users should be cautious when eating or drinking near the computer equipment. Food and drink can cause damage to electronic equipment such as keyboards.

39.1.3 Environmental Considerations

To reduce the damage done by electrical power problems, all computer workstations must use surge suppressors. Computer equipment with critical production applications must also have an uninterruptible power system (UPS).

39.1.4 Use of Personal Equipment

The Agency provides all necessary and appropriate equipment to employees to perform their job functions. Employees should refrain from bringing into the workplace their own computer, computing equipment, or electronic accessories (such as speakers, sound cards, mice, keyboards, modems, monitors, temporary radio, or Bluetooth connections of personal equipment such as cellular phones or speakers) to install into the Agency's electronic systems if there is any potential that such equipment or accessories could negatively impact or pose a security risk to the Agency systems.

Employee use of personal electronics or accessories on Agency systems is at the employee's own risk. The Agency is not responsible for damage to personal equipment or accessories caused by employee use or by incompatibility with the Agency system.

The Agency has a separate Telecommuting Agreement which governs employee use of personal equipment while working remotely.

39.1.5 Changes to Hardware

Computer equipment supplied by the Agency must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without the prior written authorization from the IT Section. Changes any computer related equipment is to be initiated through the IT Service Request form process.

39.2 Passwords

39.2.1 Choice of Passwords

Passwords are required for Agency computer systems. User-chosen passwords should be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequence such as "123456" should not be employed. Likewise, personal details such as spouse's name, license plate, social security number and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords and keys must also not be any part of speech. For example, proper names, geographical locations, common acronyms and slang must not be employed. Passwords may not be shared with friends, family or coworkers. Sharing your user ID or password with other persons is prohibited. If you share your user ID, you will be solely responsible for the actions that other persons may perform. Users may not access a computer account that belongs to another employee.

The fact that a user chooses his/her own password does not mean that the use of the Agency equipment is private as to that user. Agency may access the computer and its files at any time to verify business use or to retrieve necessary information. Passwords are required to be changed every 90-days.

Failure to provide passwords or access upon Agency request is grounds for discipline, up to and including termination of employment.

39.2.2 Storage of Passwords

Staff must maintain exclusive control of their personal passwords; they must not share them with others. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, computers without access controls or in other locations where unauthorized persons might discover them.

39.2.3 Termination of Employment

When an employee is terminated, the HR Department will immediately notify the IT Department, which will then take steps to terminate the employee's access so as to maintain security and integrity of Agency systems and equipment.

39.3 System Configuration and Software

39.3.1 Changes to Application Software

The Agency provides standard software for all users, and specialized software for certain operational activities. Users must not install other software packages on computer equipment without obtaining advance written permission from the IT Department. Likewise, staff must not permit automatic software installation routines to be run on Agency computer equipment unless the IT Department has first approved these routines in writing. Unapproved software may be removed by the IT Department without advance notice or compensation.

39.3.2 Changes to Operating System Configurations

On Agency supplied computer hardware, users must not change operating system configurations, upgrade existing operating systems or install new operating systems. If such changes are required, they will be performed by under the direction of the IT Department (in person or with remote system maintenance software).

39.3.3 Software Installation and Copying

The copying of software or installation of software that is owned by the user onto the Agency's computer system is not only against policy, it is illegal. Under no circumstances may staff bring software from home and install it on the Agency's computer system. Staff also may not copy software from the Agency's computers and take it home. Such activities violate software copyright laws and carry penalties. If software is needed for any reason, contact the IT Department.

39.4 Document Storage

The Agency's Document Management System (DMS) is to be used for the creation and storage of all Agency documents and files. The work of Agency employees is the property of the Agency and should be stored and filed in a consistent manner. In limited circumstances, documents and files may be stored in the Userdata Folder. In very limited circumstances, documents and files may be stored on a hard drive.

The use of the DMS allows for proper storage and indexing of files, as well as daily backup of information.

DMS folders are created by the IT Department. Employees requesting new folders should use the IT Service Request Form. Because documents in DMS are "searchable" by a variety of items, including actual text, the creation of folders should be kept to a minimum.

39.5 Maintaining Security

39.5.1 Browsing

Deletion, examination, copying, or modification of files and/or data belonging to other users without prior written consent of the IT Department is prohibited.

Staff must not browse through Agency computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing.

39.5.2 Tools to Compromise Systems Security

Unless specifically authorized in advance in writing by the IT Department, Agency staff must not acquire, possess, trade or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those, which defeat software copy-protection, discover secret passwords, identify security vulnerabilities or

decrypt encrypted files. Unless specific permission has been obtained from the IT Department, users are prohibited from using such tools.

39.6 Use of Internet and Email

39.6.1 Personal Use

Use of Agency computing resources for personal purposes are permissible so long as the incremental cost of the usage is negligible, and so long as no Agency business activity is preempted by the personal use. Staff must not employ the Internet or other internal information systems in such a way that the productivity of other staff is eroded; examples include chain letters, games, binary attachments, documents in excess of 3 megabytes and broadcast of bulk e-mail (direct mail marketing) and charitable solicitations. Under no circumstances may staff download and/or install any programs, personal software or video games. Staff may not tamper with the computer standardization or software-controlled system policies.

39.6.2 Email Guidelines

You agree and understand that whenever you send electronic mail, your name and user ID are included in each mail message. You are responsible for all electronic mail originating from your user ID. Forgery (or attempted forgery) of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited. Attempts at sending harassing, obscene and/or other threatening email to another user are prohibited.

39.6.3 Using the Internet

The following are ***unacceptable*** examples and uses for accessing the Internet:

- Employees will not use profanity, obscenity, or other language, which may be offensive when communicating with others.
- Employees may not use the internet for personal gain or objectives, including but not limited to financial gain, commercial purposes, or political purposes.
- Employees are not to use their access to gain unauthorized access or misuse any other systems on the Internet.
- Employees are not to jeopardize network services by distributing computer viruses or worms.
- Employees are to avoid any actions that cause interference to the network or the work of others on the network (i.e., mass chain letters).

- Employees are not to access pornographic or similar websites.
- Employees are not to access gambling or similar websites

The following are ***recommended*** uses or practices for accessing the Internet:

- Due to a lack of regulation and security in the Internet environment, employees should not give out personal information like home address, telephone numbers, and credit card numbers.
- Passwords should be kept private and should be changed frequently.

39.7 Accessing Email from a Remote Computer

Users may access the Agency's Outlook email system for their own Agency email from one of the following websites: https://mail.scvwa.org or https://office.com. Do not access this website from Agency's computers – this may cause the network to crash.

39.8 Mobile Phones

Some Agency employees are issued mobile phones for Agency use. On occasion, mobile phone calls for emergencies may be necessary, such as; illness or injury to family members, changed family plans, or for similar reasons. Employees are cautioned, however, to advise those who might call them on their mobile phone of these conditions. Excessive mobile phone use for personal or non-Agency use may result in an employee's mobile phone being removed. This policy shall apply to both phone calls and text messages.

Effective January 3, 2012, the Federal Motor Carrier Safety Administration (FMCSA) regulations prohibit Commercial Drivers from talking on a hand-held mobile phone while driving, or while stopped at traffic lights, stop signs, and traffic delays.

While hands-free use of mobile phones may be permitted when safe to do so, it is the responsibility of the employee to request and use a hands-free device for their mobile phone. Under no circumstances shall an employee send or review text messages or emails while driving.

Further, this section on mobile phone use is subject to review and revision by the Agency at any time, with or without prior notice.

39.9 No Expectation of Privacy

The Agency maintains and utilizes, as part of its operations, a computer system, voicemail, e-mail and other systems. These systems are provided to assist employees in the conduct of Agency business. All computers and the data stored on them, as well as all voicemail and the data stored on it, and all records of internet access, are and remain at all times, the property of Agency. As such, all voicemail, email, SMS or text messages, photographs, or other messages composed created, sent, and received are, and remain, the

property of the Agency. Employees maintain an obligation to provide access or assist in obtaining access to any assigned device containing such data or files. Refusal or failure to provide access or assist in obtaining access when requested is grounds for discipline, up to and including termination or employment. **No employee has any expectation of privacy regarding such messages or records.**

Agency reserves the right to retrieve and read any message or record composed, created, sent or received on the voicemail, e-mail, internet or other systems at any time, with or without advance notice to the employee.

39.10 Penalty for Violation of this Policy

Violation of this policy is grounds for discipline, up to and including termination. Employees violating this policy are acting outside the course and scope of their employment and may be personally liable for such violations.