COMPUTER OPERATING AND SECURITY – FD-IX-2

POLICY:

All OPTIONS NORTHWEST owned computer hardware, software, related equipment and telecommunications facilities (the "System") and all data and information stored, used or accessed through the System ("Data") will be maintained and kept secure.

Only those designated and approved users will have access to the organization's information technology resources. Users will employ only those computer accounts for which they are authorized and shall take all necessary precautions to prevent others from obtaining access to their computer accounts. The holder of a computer account and password is responsible for protecting the organizations information technology facilities from unauthorized access by keeping the password confidential and changing it regularly.

All resources are to be used in a reasonable and responsible manner.

PURPOSE:

To ensure security of the computer system and data is effectively maintained and monitored on an ongoing basis.

PROCEDURE:

1. The login to the system is controlled by a unique username and password. The IT Managed Service Provider assigns the username and the user's initial password.

2. The users must reset their password upon first login to the system. Their password must be eight or more characters and must include: at least one lower case letter, one upper case letter, one number and one special character.

   The password should not include the user's login name or the name of the user, their spouse/partner, children, pet, nickname, or any other names commonly known to others. It should also not be a word pertaining to OPTIONS NORTHWEST, the users work or any activity that they participate in or follow that is commonly known.

3. The username is used by the system to control which applications and directories each user can access. This is set up and controlled by the IT Managed Services Provider based on the direction of the Director, Finance and Administration or the Executive Director.

4. Only the IT Managed Service Provider, Director Finance and Administration and the Executive Director have access to all applications and all directories of all users.

5. System login will be locked upon five unsuccessful attempts in order to prevent intruders.

6. The IT Managed Service Provider and Director, Finance and Administration will be notified, and the account will be re-instated upon verification that the appropriate user was attempting to login.

7. A password reset can be requested after hours if the user has provided a personal telephone number or email address during their first login that the IT Managed Service provider can use to authenticate the reset request.

8. If it is discovered that an unauthorized user is trying to access information, a written warning will be given by the Executive Director. Computer information system access may be denied if directed by the Executive Director.

9. Each user must log off their computer when it is not in use for an extended period of time. If users are logging on to the Network through remote access or VPN, they must shut down the remote access immediately after use.

File Management

Viruses:
All software, files and attachments being accessed through our System are automatically scanned by the Network's virus scanner. However, the virus scanner is not infallible. Users will not open email attachments received from unknown third parties. If users identify a virus, worm or trojan horse, or what they suspect to be one, do not try to fix the problem. Immediately shut down the computer and contact the IT Managed Service Provider. Under no circumstances are email attachments in the form of executable programs (.exe) to be run on any computer.

Data and System Access:
Access to OPTIONS NORTHWEST Data is on a need to know basis only. Unauthorized access to the System or Data is strictly prohibited. Unauthorized access to third-party data and systems is strictly prohibited. Any form of tampering, including hacking, is strictly prohibited. If users identify a new way to access information, they are to report it to the Director, Finance and Administration or the Executive Director. Obtaining or trying to obtain other user's passwords or using programs that compromise security in any way is strictly prohibited. Destruction, theft, alteration, or any other form of sabotage of the System and Data or any third party's system or data is strictly prohibited. To safeguard against hackers, users are to never give any information about our System to

third-parties. If someone requests such information, report the incident immediately to IT Managed Services Provider.

Data Storage:
All Data must be stored on OPTIONS NORTHWEST's local area network ("the Network") by utilizing "OneDrive' Storing information on your desktop or laptop computer is not recommended, except when users are unable to be connected to the Network. Once users are able to be reconnected to the Network, they will ensure all data is transferred to the Network.

Use of Personal Devices:
Personal mobile or computer devices (including, but not limited to, personally owned cell phones, tablets, laptops and computers) can be used to access the employee's work email account under the following conditions:

- Each device that is used to access company information must have a PIN, password, passcode, or other security measure in place that automatically locks the device when it is not in use;
- Email accounts can be accessed through webmail by viewing it directly in a web browser such as Chrome, Explorer, Safari, etc, or by downloading the Outlook App on the personal device and connecting the email account through the App. Other email applications, such as Apple's Mail App, cannot be used to access the work email address;
- Upon termination of employment, the IT Managed Service Provider will remotely remove all email content from the device; and
- If the personal device is lost, stolen, hacked or damaged, the employee is expected to immediately notify the IT Managed Service Provider to remotely remove all email content from the device to prevent access by unauthorized parties.

Software:
OPTIONS NORTHWEST does not own computer software, but rather licenses the right to use software from third parties. Accordingly, licensed software may only be reproduced by authorized personnel in accordance with the terms of the software licensing agreements. Unauthorized copying, modifying, redistributing and republishing of copyrighted or proprietary material are strictly prohibited.

Unauthorized Changes to your Computer:
Installing software or making changes to computer hardware, software, system configuration and the like are strictly prohibited, without prior authorization from the Director, Finance and Administration or the Executive Director.

Employee Privacy:
OPTIONS NORTHWEST reserves the right, without prior notice to access, disclose, use, or remove both business and personal computer communications, files and information on a user's computer or in the Network. Random audits to verify compliance with this Policy may be performed. OPTIONS NORTHWEST will investigate complaints about violations of this Policy by employees. OPTIONS NORTHWEST may monitor Internet activity to see what sites are frequented, duration of time spent, file downloads, and information exchanged.

Email
The use of OPTIONS NORTHWEST email system is to carry out user's employment duties. The same standards of decorum, respect and professionalism that guide employees generally in the office environment, including letter writing and telephone communications, apply equally to email communication.

Internet:
Internet connections with the exception of OPTIONS NORTHWEST open WiFi connections, are authorized for specific business needs only. Without limitations to the foregoing, the following activities are prohibited.

- Downloading information of any kind, including data, files, programs, pictures, screen savers, and attachments except as is required in the course of user's employment duties and in compliance with all laws; and

- Accessing inappropriate websites, data, pictures, jokes, files, games, including without limitations, gambling sites, sites containing pornographic material, chat rooms and bulletin boards.

Tracking Usage:
OPTIONS NORTHWEST reserves the right to track and log internet usage and to revoke or suspend internet access at any time.

RECOMMENDED BY: Director, Finance and Administration **APPENDICES:** 0

OPERATIONAL ACCOUNTABILITY: Administration, Finance, Human Resources, Community Services Administration, Community Services (all)

ORIGINAL POLICY DATE: July 1993

AUTHORIZED BY: Executive Director **SIGNATURE:**