COMPUTER USAGE POLICY **SECTION 5.24**

Sandusky County computers and information systems are County Property. Employees are strictly authorized to use the computers and information systems only for work purposes. Employees have no right to privacy with regard to the Internet and email on County systems. Sandusky County reserves the right to examine all data stored or transmitted by their computers and systems. Without notice SCAA may enter, search, monitor, track, copy and retrieve any type of electronic files of any employee or contractor. These actions may be taken for business purposes inquiries including but not limited to theft investigation, unauthorized disclosure of confidential business of proprietary information, excessive personal use of the system, monitoring work flow and employee productivity and public records requests.

No County employee may install, uninstall, or reconfigure any software or hardware owned by the county without prior authorization from the County. The use of privately-owned or contractor-owned devices is strictly prohibited. Prior authorization is necessary to obtain email on a personal device.

A. Allowable Uses of Computer and Information Systems for Business Purposes.

1. Facilitating job function performance.

2. Facilitating and communicating business information within the County network.

3. Coordinating meeting locations and resources for the County.

4. Communicating with outside organizations as required in the performance of employee job functions.

B. Prohibited Uses of Computers and Information Systems, Including But Not Limited to E-mail, Instant Messaging, and the Internet

1. Violating local, state, and/or federal law.

2. Harassing or disparaging others based on age, race, color, national origin, sex, sexual orientation, disability, religion, military status or political beliefs. Harassment and disparagement include but are not limited to slurs, obscene messages, or sexually explicit images, cartoons, or messages.

3. Threatening others.

4. Soliciting or recruiting others for commercial ventures, religious or political causes, outside organizations, or other matters which are not job related.

5. Using computers for information systems in association with the operation of any for-profit business activities or for personal gain.

6. Sabotage, e.g. intentionally disrupting network traffic or crashing the network and connecting systems or intentionally introducing a computer virus.

7. Vandalizing the data of another user.

8. Forging electronic mail and instant messenger messages.

9. Sending chain letters.

10. Sending rude or obscene messages (anything that would embarrass or discredit the County).

11. Disseminating unauthorized confidential or proprietary County documents or information or data restricted by government laws or regulations.

12. Browsing or inquiring upon confidential records maintained by the County without substantial business purpose.

13. Disseminating (including printing) copyrighted materials, articles, or software in violation of copyright laws.

14. Accessing the Internet in any manner that may be disruptive, offensive to others, or harmful to morale.

15. Transmitting materials (visual, textual, or auditory) containing ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on age, race, color, national origin, gender, sexual orientation, disability, religious or political beliefs.

16. Sending or soliciting sexually-oriented messages or images.

17. Using the Internet or instant messenger for political activity.

18. Using the Internet to sell goods or services not job-related or specifically authorized in writing by an approving authority.

19. Downloading and viewing non-work-related streaming audio or video (i.e. listening to radio stations, etc.) due to the limited bandwidth of the system.

20. Intentionally using Internet facilities to disable, impair, or overload performance of any computer system or network or to circumvent any system intended to protect the privacy or security of another user.

21. Speaking to the media or to the public within any news group or chat room on behalf of the County if not expressly authorized to represent the County.

22. Uploading or downloading games, viruses, copyrighted material, inappropriate graphics or picture files, illegal software, and unauthorized access attempts into any system.

C. **Use of the World Wide Web:** The Internet is a powerful and useful tool for research and other functions. Employees are encouraged to develop computer and Internet skills to improve their job knowledge and to promote the interests of the appointing authority's office. Employees should treat the Internet as a formal communications tool similar to the telephone, radio, video, and written communications. All employees are responsible for their actions and communications using computers and the Internet. All employee activity online via the use of County computers and devices may be monitored at any time.

D. **Remote Access:** SCAA will determine employees who it is necessary to have remote access. SCAA along with Sandusky County IT reserves the right to limit access to remote access.

In an effort to minimalize the threat of cybersecurity issues, the following guidelines will be enforced:

1. Only those who have a county owned computer or device will be able to utilize remote access.
2. Two factor authentication will be required on all remote access points
3. All devices requiring remote access must have currently supported, up-to-date operating systems and endpoint protection.
4. All remote access requires connectivity via the county's secure VPN with 2FA/MFA.

E. **Breach Procedure:** In any case in which an employee feels their system has been compromised and a possibility that a suspected breach has occurred, the following steps should be taken immediately:

1. Report immediately to your department head and IT.
2. Turn off your computer and unplug when possible.
3. Wait for IT to respond to assess the situation

Any violation of this policy or other improper use of the Employer's information systems (computers, e-mail, Internet, etc. shall result in discipline up to an including termination. The level of discipline will be based on the seriousness of the violation and the employee's discipline record.