

COMPUTER RESOURCES ACCEPTABLE USE POLICY
Adopted 7/13/04 – Amended 5/28/2024

1. PURPOSE

- 1.1 To adopt and enforce a policy that addresses the acceptable use of computer resources (user ID's, passwords, access privileges, computers, servers, peripherals, hardware, applications, programs, software, data, files, information, internet, email, communications, Local Area Network, Wide Area Network) at Tuscola County.
- 1.2 To assure that Tuscola County computer resources are utilized for the business of government work as it relates to a user's job function.
- 1.3 To protect the users and the computer resources of Tuscola County from illegal or damaging actions by individuals, either knowingly or unknowingly. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.
- 1.4 This policy will be presented to all employees upon acceptance of employment. This policy will be disseminated to all County workstation desktops.

2. SCOPE

- 2.1 This policy applies to employees, contractors, consultants, temporaries, and other workers at Tuscola County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Tuscola County.

3. POLICY

- 3.1 It is the policy of the Tuscola County Information Systems (I.S.) Department to not actively monitor the content of a user's Personal Computer (PC). However, any computer resource within the scope of responsibility of the I.S. Department may be monitored and/or audited when it is deemed appropriate. Data created on any I.S. equipment, software or network is property of Tuscola County.
- 3.2 Use of computer resources is restricted to the user's job function within the County government.
- 3.3 Users are not permitted to share their login IDs and/or passwords.
- 3.4 If a user suspects that an ID, password, or computer resource has been compromised or hacked, they must immediately notify the I.S. Department so that appropriate action can be taken.
- 3.5 Users are not permitted to knowingly modify, delete, move, copy, or exchange any file/program/data/information that will harm or disrupt computer resources.
- 3.6 Users are not permitted to knowingly distribute viruses or exchange harmful programs/files.
- 3.7 The I.S. Department maintains the right to block access to any internet resource deemed inappropriate. Internet resources will be monitored and controlled.
- 3.8 Utilizing internet resources to access pornographic material, web surf, shop, game, play, streaming media, micro-blogging, gamble, chat, file share, peer-to-peer network (P2P), virtual private network (VPN), connect to non-County email systems, instant message, or any other inappropriate use is not permitted.
- 3.9 Users are not permitted to purchase, install, or dispose of any networking device, computer software/hardware, or peripheral equipment without authorization from the I.S. Department.
- 3.10 Users are not permitted to use non-I.S.-issued software/hardware on any network, with the exception of the Employee WiFi Network, which has no access to the core networks.
- 3.10b The Tuscola County WiFi Network is for Employees ONLY. Any observed access by visitors or the public must be reported to the I.S. Department immediately. Handing out the WiFi password to non-County Employees is strictly prohibited.
- 3.11 Any users initiating banking transfers on behalf of Tuscola County, must do so from I.S. approved device. This machine will be limited to only banking activity. Only authorized personnel will be given access to banking devices.
- 3.12 Users are not permitted to open, modify, delete, move, copy, or exchange any file/program/data/information that are not related to their job function within the County government.
- 3.12b Users who knowingly have access to data/programs/modules/information they are not authorized to access must report the inappropriate access immediately to their supervisor and the I.S. Department.
- 3.13 Users are not permitted to exchange, divulge, or grant access of any file/program/data/information with unknown sources or sources that have no direct working relationship with the function of the County government.
- 3.14 Users are not permitted to use computer resources to create, exchange, or display any harassing, offensive, pornographic, or other inappropriate material. This includes sending unsolicited bulk email, spam, and chain letters via email.
- 3.15 Users are not permitted to utilize computer resources for illegal purposes that are in violation of any federal, state, or local law.
- 3.16 Users are not permitted to utilize computer resources to violate any Tuscola County policy.
- 3.17 Violations of the rights of any person or company protected by copyright, trade secret, patent or intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Tuscola County are strictly prohibited.
- 3.18 Circumventing user authentication or security of any host, network, or account is strictly prohibited.
- 3.19 Use of non-county email services, such as AOL or Yahoo on Tuscola County's network is prohibited unless authorized by I.S. Any email conducted with the use of the @tuscolacounty.org domain, shall remain professional in manner and never for personal purposes. All email should be treated as public record.
- 3.20 Users must complete I.S.-approved Security Awareness Training at the time of employment and once a year. They are also subject to monthly phishing simulation emails performed by the IS department. It is the user's responsibility to ensure that this training is completed.
- 3.20b Users failing monthly phishing simulation emails must retake the Security Awareness Training within *five* working days of each instance of failing the simulation. If training is not completed within *five* working days, all network access will be revoked until training has been completed.
- 3.21 Any technology-based items not covered by the above policies are denied unless previously discussed and approved by the I.S. Department.

I Acknowledge that I have read, understand, and agree to the Computer Resources Acceptable Use Policy

Signature: _____ Date: _____