Title: Acceptable Use Policy
Policy Number: 804
Effective Date: November 29, 2024
Authorized by: Pottawattamie County Board of Supervisors

1.0 Purpose

This policy defines the acceptable use of computer systems and networks under the control of Pottawattamie County and its affiliated departments. This policy is designed to protect the Employee and Pottawattamie County computer systems and networks by ensuring appropriate use of resources and equipment. Inappropriate use increases exposure to risks including virus or malware attacks, compromises of computer and network systems, legal issues, and degraded performance.

2.0 Scope

This policy applies to all Employees, contractors, consultants, temporary Employees, and any other workers or guests at Pottawattamie County. This policy applies to all equipment that is owned or leased by Pottawattamie County and its affiliated departments.

3.0 Policy

3.1 General Use and Ownership

1. While Pottawattamie County's network administration desires to provide a reasonable level of privacy, Employees should be aware that any data they create on the corporate system remains the property of Pottawattamie County and therefore remain subject to data disclosure requests and compliance audits. Because the need to protect Pottawattamie County's network, confidentiality of information stored on any network device belonging to Pottawattamie County cannot be guaranteed.
2. The Pottawattamie County Information Security team recommends that any information that an Employee considers sensitive or vulnerable be encrypted.
3. Employees are responsible for exercising good judgement regarding the reasonableness of personal use. Individual departments are responsible for creating additional guidelines concerning personal use of Internet/Extranet/Intranet systems. In absence of such policies, Employees should consult their Supervisor or Department Head.
4. For security and network maintenance purposes, authorized individuals with Pottawattamie County may monitor equipment, systems and/or employee's network traffic, and data usage at any time.
5. Pottawattamie County reserves the right to audit the network and any systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information

1. Keep passwords and user accounts secure, they should not be shared. Authorized users are responsible for the security of their passwords and accounts and any activities that are associated with them.

2. Agree to handle and protect all information stored on a computer or downloaded to portable media or hard copies with appropriate care as to prevent unauthorized disclosure or dissemination of the information.
3. Employees must use extreme caution when opening email attachments or external media devices received from unknown senders or other third parties as they may contain viruses, malware, or other vectors of attack that can compromise security, systems, and protected information. Employees must immediately contact IT if they believe they may have opened a "suspect" email by mistake.

3.3 Unacceptable Use

The following activities, in general, are prohibited. Some employees and systems may be exempted from these restrictions due to the nature of their legitimate job duties. Under no circumstances is an Employee of Pottawattamie County authorized to engage in any activity that is considered illegal under local, state, federal, or international law while using resources owned or operated by Pottawattamie County.

The following list provides a framework for activities that fall under the unacceptable use category. This list is neither exhaustive nor all-encompassing, any questions regarding on the acceptability of use should be directed to the **INFORMATION TECHNOLOGY DEPARTMENT** for clarification.

3.4 Systems and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Usage of information resources must not constitute a conflict of interest. Personal business or use for personal gain constitutes a conflict of interest.
2. Using information resources in a manner that jeopardizes the confidentiality, integrity, or availability of Pottawattamie County information resources.
3. Any form of harassment, nuisance or spam, or other malicious activities while using Pottawattamie County's systems, resources, or intellectual properties.
4. Using non-Pottawattamie County owned, leased, or authorized equipment to store, process, or transmit non-public information.
5. Providing lists of Pottawattamie County systems, networks, or users and employees to parties outside of Pottawattamie County for purposes other than legitimate business necessity.
6. Revealing your passwords to others or allowing use of your accounts by others. This includes family and other household members when working remotely.
7. Circumventing user authorization or security of any host or system, network, or account; cloning, spoofing, or bypassing any smart cards, proximity cards, or any other means of alternative forms of authentication.
8. Accessing, or attempted access, of any system or information that is not intended for your use or accessibility.

9. Port scanning, security scanning, network monitoring which will intercept data not intended for the Employee's workstation, vulnerability and penetration testing is expressly prohibited unless prior notification has been given to, and approval requested from, the Pottawattamie County Information Security team.
10. Violations of any trademark, copyright, trade secret, patent, or any other intellectual property rights. This includes uploading, downloading, distributing, and/or installing any product or software that are not appropriately licensed or have formalized agreements with Pottawattamie County.
11. Establishing shadow networks, infrastructure, or rogue wireless access points to bypass or extend the Pottawattamie County network beyond the management of the appropriate agencies control.
12. Introduction of malicious programs into the network or servers, such as viruses, malware, trojan horses, etc.
13. Installation of any software that has not been pre-approved and scanned for viruses or malicious payloads is strictly prohibited.
14. Uploading or sharing non-public data into publicly available generative AI (see Information Classification Guide on the Employee Portal for classifications and how to handle each) is strictly prohibited.
15. This list is not exhaustive. If you have any questions about an activity, please contact your Supervisor or Department Head.

4.0 Non-compliance and Enforcement

Violations of this county policy puts the County at risk for regulatory fines or loss of system access. Additionally, violating this policy may put the County information systems at risk for data loss or compromise.

Pottawattamie County reserves the right to restrict systems and users access to network resources upon discovery of security incidents or breaches, behavior that is affecting the network availability and stability, or any other events that put resources in jeopardy and will work with the appropriate departments regarding a permanent response.

Any user who knowingly violates these policies may be subject to disciplinary action following the *Pottawattamie County Employee Handbook* guidelines.

Revision History: Initial Effective Date May 10, 2022. Revised by Policy Committee November 12, 2024.
Board Approval: November 19, 2024