Title: End User Security
Policy Number: 805
Effective Date: June 25, 2019
Revision Date: July 5, 2022, November 22, 2022
Authorized by: Pottawattamie County Board of Supervisors

Purpose

This document defines the end user security policy for information systems under the control and responsibility of Pottawattamie County, their departments, and personnel. This policy is designed to provide guidance for users of information systems ensuring compliance with all established legal guidance.

Scope

This policy applies to all information systems and applications owned and/or operated by or on behalf of Pottawattamie County. All employees, vendors, and contractors are expected to understand and follow this policy.

Definitions

This section provides definitions used throughout the policy to ensure a common language is in use and is understood what the term means.

End User

The term end user refers to any person who uses technology to access County data and systems. This includes, but is not limited to: County employees, vendors, and contractors.

Information Asset

The term information asset refers to a particular type of data or information. Some examples of information assets include:

- Credit card number
- Citizen demographic information: name, address, and phone number
- Vendor contracts

An information asset may be stored in a digital form (spreadsheet, database, etc.) or in physical form (paper, optical disc, or magnetic tape).

Information Security Team

Information security team is not a formal committee but consists of members of the IT Department which at minimum include the CIO, IT Supervisor, and Cybersecurity Analyst.

Information System

The term information system refers to software or computer hardware that helps manage, store, organize, and/or analyze information assets. Common examples of information systems include:

- Email systems
- File storage systems
- Database servers
- Desktop or laptop computers

Information systems may be physical computers, virtual systems, or cloud-based systems.

Information Asset Owner
The information asset owner is the department or person responsible for the information asset. The information asset owner provides guidance on the classification of a particular information asset.

Malware
Malware is software that is harmful to the security or normal operations of an information system. Malware includes common issues such as computer viruses or ransomware. Information systems with malware may be used to steal information, spy on users, or disrupt normal operations of applications. The use of anti-malware software helps ensure the information systems are protected and any malware found can be removed from a system to return the system to normal operations.

Policy
All users and information systems at Pottawattamie County are required to adhere to minimum security controls as defined in this document. This policy provides guidance and requirements for all users to ensure the information assets are appropriately controlled. Users are limited to approved hardware and software.

Minimum Security Requirements
Expectation of Privacy
Users should assume all activity is monitored while using County information systems including network and internet access. All activities involving County information systems and associated assets are subject to logging and monitoring by authorized personnel within the Information Security Team or by automated systems. All digital communications are property of the County, and many forms of communication may be classified as *Public* (see Information Classification Guide on the Intranet for classifications and how to handle each). The monitoring includes, but is not limited to, web sites visited, emails (both sent and received), chat messaging, and files transferred, camera and door access control records. The monitoring activities are required by multiple federal and state statutes.

Users of County information systems should have no expectation of privacy beyond the minimums guaranteed by law or defined within these policies (attorney/client privilege, criminal investigation, etc.).

Physical Security Considerations
All physical hardware (laptops, desktop, removable media, and mobile phones) and non-public hard copy documents are at risk for theft, damage, or information loss if left in an insecure location. All physical hardware and non-public hardcopy documents must be secured if they are going to be left unattended. Examples of security mechanisms include the following:

- Stored in a secured Pottawattamie County office
- Stored in a secured residence away from easy outside access
- Carried on a Pottawattamie County employee or contractor’s person

Credential Management
Credentials management refers to account identification information. Typically, this involves a username identifying a particular user of the information. The username should be unique and assigned to a

particular user. The standard for Pottawattamie County accounts is to assign each user account to exactly one user. A user may have multiple accounts (if needed for their job role), but accounts should not be shared. If a shared account is needed for a legitimate business purpose, the IT Department must be contacted for an approved exception to this policy. All exceptions must be approved in writing by the Chief Information Officer. Exceptions are reviewed on a periodic basis to ensure the exception is still required. To authenticate a particular username, an authentication mechanism is required. The most commonly deployed authentication mechanism is a password for the user account. All passwords must meet the following minimum requirements:

- Minimum length
- Complexity (3 of the following 4 categories must be met):
    - Upper case alphabet characters
    - Lower case alphabet characters
    - Numbers
    - Symbols

For systems part of the local domain, the password characteristics are automatically enforced. For passwords in other applications or systems, the account holder is responsible for ensuring the password characteristics should be used (even if not required by the system).

The use of multi-factor authentication (MFA) is required where available. MFA refers to an authentication process using multiple distinct components such as:

- Something the user knows (a password or PIN for example)
- Something the user is (biometric details such as fingerprints)
- Something the user has (such as their mobile phone or authentication token)

In order for the MFA to be implemented properly, the factors must be independent of each other, and more than one method must be used simultaneously for a particular user account. See Appendix A for specific MFA-related details.

Credential information (username and credentials) should not be stored except in an approved solution.

When a user has left County employment or has been placed on extended, involuntary leave, the department manager must notify the IT Department within 24 hours to disable the user's account. For voluntary leave, greater than 30 days, the department manager should consult with the IT Department as soon as possible to determine if the user's account should be disabled. If the user has been separated from employment, access to the user's information assets (such as email and file storage) can be provided to the department manager or other designated user.

If a user changes roles (either within or between departments), the department head must notify the IT Department as soon as possible to ensure the appropriate rights have been assigned to the user and any rights no longer needed are removed.

Minimum Security Requirements

All information systems accessing the applications, network, and information systems at Pottawattamie County must meet a set of minimum-security requirements. The purpose of these requirements is to ensure the safety, security, and availability of the information assets and resources deployed at Pottawattamie County. If these components are not properly secured, the services and information provided to the citizens may be adversely impacted.

Malware Protection

To maintain protection against common malware, all information systems should have current, managed, installed, and operating anti-malware installed. **Error! Reference source not found.**The anti-malware system must be updated automatically and on a regular basis to ensure the software will protect the information system from new and emerging threats to the environment preventing risk of compromise, loss of service, and/or damage.

Operating System and Application Patches

Operating Systems and Applications Patches require regular patching to ensure flaws are corrected and information systems are protected. Operating Systems and Applications must have patches as soon as reasonably possible.

Communications Methods

Communicating with employees, members of the public, and vendors must follow regulations such as the Freedom of Information Act (FOIA) or Iowa Open Records Codes. To ensure Pottawattamie County complies, only approved communications applications and methods may be used to conduct official business.

Electronic Messaging

Electronic Mail (email) services are provided and maintained by the IT Department. Employees are not allowed to forward non-public information to personal or public accounts except for your own personal information.

All text messaging used for Pottawattamie County business must follow the *Mobile Device Policy found in the Employee Handbook*.

Social networking should not be used to send non-public information following department policies.

Secure Communications

When using communications methods for sharing non-public information, encryption needs to be enabled to ensure the information assets are appropriately protected.

File Sharing

When sharing files with others, care must be taken to ensure the recipient should have access to the information and that the information is being shared appropriately. When sharing with external people or organizations, the information being shared needs to be appropriately protected.

Remote Access Solutions

Users requiring remote access will use the IT Department installed and configured virtual private network (VPN) solution.

Removable Media Encryption

The use of removable media requires device-level encryption.

System Procurement Process

To ensure compatibility with County systems, the IT Department must be involved at the beginning of

the procurement cycle for new hardware and/or software. The purchase of the solution will follow requesting department's policies.

Information Destruction

Digital media no longer in use by County Departments will be given to the IT Department for destruction.

Auditing and Compliance

The IT Department is responsible for auditing the environment. These audits include, but are not limited to, logging user activities, inspecting traffic into and out of the environment, and ensuring policies are followed. The audit process may be either automated (such as the collection and analysis of log information) or in person. These audits may lead to configuration, policy, or procedural changes.

Non-Compliance

Violations of the County policies put the County at risk for regulatory fines or loss of system access. Additionally, violating the policies 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 will be subject to disciplinary action following the *Pottawattamie County Employee Handbook* guidelines.

Appendix A – Multi-Factor Authentication

Purpose

Multi-Factor Authentication (MFA) is achieved when multiple forms of authentication are used to increase the likelihood that the credentials are from the individual to whom they were assigned. This process reduces the risk of impersonation or the use of compromised credentials by an unauthorized individual.

MFA is required to be used by all Pottawattamie County users with network access to County systems. MFA is achieved using a special one-time passcode (OTP) authentication generated from an approved hardware token (fob) or smartphone application, in addition to their Windows credentials.

Definitions

Fob

An IT-issued device used to generate a one-time passcode.

OTP

One-time passcode.

OTP Device

The device that is used to generate one-time passcode. This refers to both fob and smartphone.

Smartphone OTP App

Authorized and managed smartphone app that is used to generate OTP.

Policy

1. When authenticating using MFA all users must use the generated OTPs from their smartphone app or approved hardware token (fob) as a second factor security login, in addition to their Windows credential.
2. Only smartphones using the associated app or hardware tokens (IT-provided fob) may be used for OTP generation.
3. If using the smartphone app, users must notify the IT Department when they change their smartphone device, even if they keep the same phone number. IT can assist users with the process of registering their new smartphone device.
4. In the event a device becomes lost, even if its last known location is believed to be secure, immediately inform IT and the factor will be temporarily disabled and another factor or temporary access code will be issued to ensure that the lost device is not used to compromise the user account. If the device is unrecoverable, IT will assist in permanently changing the user's device settings. The cost to replace a fob is $25, to be charged to the employee's department.
5. Devices must be properly secured, not shared.
6. Users are expected not to leave their OTP devices unattended in a public place.
7. Users should not mark their hardware fobs or smartphones with any identifying information such as name, username, password, or any reference to Pottawattamie County systems.

Factor Choices

Smartphone

1. User is responsible for furnishing his/her personal smartphone, or a County-issued smartphone. Pottawattamie County will not issue smartphones exclusively for users to use as MFA devices.
2. The County IT Department only supports the OTP app, not the smartphone itself. Each user is responsible for making sure his/her smartphone is in working condition. Pottawattamie County is not responsible for the cost of repairing or replacing the personal smartphones used as OTP devices or for any costs associated with data plan usage.
3. The approved OTP app must be installed and used to generate the OTP.
4. Users are expected to leverage the electronic security provided by their smartphones, including but not limited to use of a screen lock utility to access their smartphones (e.g., PIN, Password, or biometric such as a fingerprint scan).
5. Users agree to uninstall the OTP application once their need to use it expires.

Hardware Token (fob)

1. Users must take reasonable care for the hardware token (fob) which is assigned to them. Reasonable care includes, but is not limited to:
   - Protecting from water/moisture. Fobs are not water resistant.
   - Protecting from loss or theft.
2. Users are expected not to transport their OTP fobs in the same bags as laptops that are used to access Pottawattamie County systems.
3. In certain instances, a user may be assigned a specific type of hardware fob that plugs into the USB port of a device. It is critical that these fobs are not left unattended in the device or stored with the device. Failure to properly store and use the fob will result in the loss of access to a USB fob.
4. Users are expected to return their hardware tokens (fob) to their supervisor when they terminate their employment with Pottawattamie County or no longer have access to any of the systems that require MFA.

Contingency Access

1. In situations when a user does not have their fob or smartphone and needs access, the user must contact the IT Department for a temporary OTP. MFA users can contact the IT Department during normal business hours to request temporary OTP when they don’t have their OTP device to authenticate.
2. Once a user’s identity has been verified an Access Code will be generated and they will be given a code to access County Systems.