Kenton County Fiscal Court

Kenton County, KY

KENTON COUNTY
TECHNOLOGY SERVICES

Technology Services
Policies and Procedures Manual

Originally Published: December 18, 2002

Updated: March 17, 2021

1. TABLE OF CONTENTS

1. Introduction

1.1 General

This document contains Technology Services policies and procedures applicable to all users of the Kenton County Fiscal Court data network. It provides guidance about security policies and identifies specific procedures that users of the network are expected to follow. The document describes a comprehensive approach to information security ensuring that managed assets (hardware, software, and data) are protected against destruction, loss, unauthorized access, unauthorized change, or disruption.

1.2 Objective

The Policies and Procedures in this document expect to accomplish the following:

- Demonstrate management commitment and support to information security.
- Assure proper implementation of security controls within the computing environment.
- Document acceptable use practices for Technology Services equipment and services.

1.3 Applicability

The Policies and Procedures listed within this document are applicable to all network users. Questions concerning the content of this document will be directed to either the employee's or the contractor's immediate supervisor or the Kenton County Fiscal Court's Director of Technology Services.

1.4 Computer Equipment and Data Ownership

All computer equipment obtained by Kenton County and/or one of its agencies is considered the property of Kenton County and/or that agency and will be used solely for Kenton County business. No personal computer equipment or computer software will be installed on Kenton County computers or its data network with the exception of personal cell phones and/or tablet devices. Personal cell phones and/or tablet devices may be configured to access the Kenton County Fiscal Court Email and Calendar programs.

All data residing on county-owned computer equipment is the property of Kenton County and can be accessed by appropriate county officials at any time. Please refer to sections on data privacy, software compliance, auditing, workstation security, procedural security and email for data privacy clarifications.

2. Security Organization

2.1 Roles and Responsibilities

Kenton County Fiscal Court is responsible for providing leadership, policy direction, and technical support to multiple agencies of Kenton County. This broad statement of responsibility encompasses information resource functions such as data center operations; voice, data and video communications; application development; data security and administration; computer and data communications hardware specifications and installation; and end user support services.

2.1.1 Data Owners

All data files and applications belong to an owner. Data owners are responsible for:

- Working with administrators, security, and network personnel to ensure access to the data and application(s) is limited to those with a legitimate business reason;
- Ensuring that security measures and standards are implemented and enforced;
- Establishing measures to ensure the integrity of the data and the applications;
- Permitting individuals' appropriate security access levels (read, write, update, etc.) for data and application(s);
- Periodically reviewing security access levels to confirm appropriateness;
- Assuring a process is in place to retain or purge information according to record retention schedules as set by the Kentucky Department of Library and Archives (KDLA); and
- Determining the sensitivity and criticality of data and application(s) based on established Federal, State, and organizational definitions.

2.1.2 Director of Technology Services

The Director of Technology Services of Kenton County or his/her designee is responsible for ensuring:

- Reasonable security measures are in place to protect data against unauthorized access or use;
- System resource usage is managed and monitored;
- Alleged security violations are responded to and problems are investigated;
- Appropriate security controls are being followed;
- Authorized individuals are approved for remote Virtual Private Network access;
- Cooperation with departments, branches, or Agencies and law enforcement in the course of an investigation of alleged violations of policy or law;
- The administration of the computing network;
- The administration of the building access control system(s); and
- Proper disaster recovery processes and procedures are in place and routinely tested.

2.1.3 Authorized Users

Authorized Users are responsible for:

- Complying with these policies, procedures and any applicable laws regarding systems and data;
- Asking questions when in doubt;
- Not subverting or attempting to subvert security measures; and
- Reporting any potential violation of these policies to an immediate supervisor and to the Kenton County Fiscal Court Director of Technology Services.

2.1.4 Directors, Managers and Supervisors

Directors, Managers and Supervisors are responsible for:

- Creating, disseminating and enforcing conditions of use for facilities and data applications under their control;
- Monitoring the use of computer resources;
- Responding to concerns regarding alleged or real violations of these policies;
- Communicating additions and terminations of employees to ensure proper addition/deletion of user access; and
- Taking appropriate disciplinary action for violation(s) of these policies.

2.1.5 Network Engineer/Administrators

Network Engineer/Administrators are responsible for:

- Taking action to assure authorized use and security of data, networks, and communications;
- Responding to questions relating to the appropriate use of system/network resources; and
- Providing advice regarding the development of conditions of use or authorized use procedures.

3. Policies and Procedures

Information is a valuable asset that must be appropriately protected against all forms of unauthorized access/use, disclosure, modification, destruction, or denial. Security controls must be sufficient to ensure the confidentiality, integrity, and availability of data stored on computer resources.

Each Kenton County agency is required to determine proper levels of protection for its information and that necessary safeguards are in place. Information that is considered sensitive and/or critical requires more stringent controls.

SUBJECT AREA: SECURITY

***Policy*:** The Kenton County Fiscal Court Technology Services Department is the custodian of Kenton County data. All information processed and stored on computer resources must be protected in accordance with its designated sensitivity or criticality.

Scope: This policy applies to all Kenton County Fiscal Court Technology Services network users who process or store computerized data relevant to agency business on a Kenton County Fiscal Court Technology Services maintained personal computer, server, or electronic storage device.

Policy/Procedure Maintenance Responsibility: The Kenton County Fiscal Court Technology Services Department is responsible for the maintenance of this policy and its revisions.

Applicability: All Kenton County Fiscal Court Technology Services network users will adhere to these policies and procedures.

3.1 Software Security

3.1.1 Overview

Software must be sufficiently protected and monitored to prevent unauthorized use, copying, modification, deletion, destruction, or denial. Software will be installed in such a manner as to prevent general system users the capability to view password or access control tables, bypass security mechanisms, or use restricted security software functions.

Access privileges to modify software will be restricted to authorized Kenton County Fiscal Court Technology Services personnel only.

3.1.2 Security Software

Security software must provide user identification, authentication, data access controls, integrity, and audit controls. Only security software approved by the Kenton County Fiscal Court Technology Services Director may be used for securing Kenton County information systems.

Security software must be adequately tested to confirm functionality and to ensure that it is minimally disruptive to associated operating systems, communications, applications, and other associated software

systems. Contractual provisions must also ensure that a vendor's software by design or configuration will not introduce any security exposures.

Vendor supplied software, e.g., operating systems, database management, communications, must be used as the primary source of security and can be supplemented, as needed, by customization. Customized and third-party add-on security software shall be used to supplement lack of built-in security features in order to meet Kenton County Fiscal Court Technology Services requirements.

All projects will include a detailed overview outlining planned access, authentication and security controls for a software system whether the software is provided by a third-party vendor or custom-developed by Kenton County Fiscal Court Technology Services programming staff.

3.1.3 Software Copyright

All Kenton County network users must comply with national, international, and commercial software license laws regarding the proper acquisition, use, and copying of copyrighted software. Using County licensed software for personal business activities in a commercial manner is grounds for disciplinary action up to and including termination of employment.

The Kenton County Fiscal Court Technology Services Department is responsible for periodically reviewing compliance with software licenses and copyright policies.

3.1.4 Software Protection

All computing devices will be scanned for computer viruses and malware. Webroot, ESET and AppRiver are used for virus and malware scanning.

3.1.5 Software Access Control

Wherever possible, resource restrictions that never allow users to request information or functions for which they do not have access (restricted menus, database views, and network devices) should be implemented by software administrator.

3.1.6 Virus Protection Procedures:

All county agency employees, contractors, and third parties accessing the Kenton County computing environment must avoid situations which increase the risk for virus infection. All files must be scanned prior to access. Reasonable precautions must be taken to prevent the possibility of virus, malware, or ransomware infection.

Only approved software is allowed to reside on Kenton County maintained computer resources. Authorized individuals of the Kenton County Fiscal Court Technology Services Department and/or third party vendors contracted by the Kenton County Fiscal Court Technology Services Department will install software.

The following steps are required:

Step 1. All files, including externally supplied media, must be checked for viruses when loaded on any computing device.

Step 2. Routine full scans of all files on servers and workstations, as well as data updates and software upgrades, will be scheduled and performed regularly, at least weekly.

Step 3. Disaster recovery plans work hand in hand with anti-virus procedures. Because backup data can become infected, the Kenton County Fiscal Court Technology Services Department has implemented a

multi-site disaster recovery process to ensure data can be retrieved, as needed, from off-site and out of region data centers.

3.1.7 Virus Removal/Notification:

If a virus-scanning program detects a virus and/or if users suspect infection by a computer virus, they must immediately stop using the involved computer and notify the Kenton County Fiscal Court Technology Services systems administration staff. The systems administration staff will ensure that the anti-virus software on the computing device is brought up-to-date, a full scan performed, and necessary disinfection procedures are executed.

The systems administration staff will immediately disconnect the infected machine from all networks. The machine will not be reconnected to the network until systems administration staff can verify that the virus has been removed. If it cannot be removed, all software on the machine will be deleted. Software will then be reinstalled and re-scanned for viruses.

3.1.8 Software Development or Installation

Security features for safeguarding information must be included in the design or implementation of applications and systems. Security controls must be documented and provided to the Kenton County Fiscal Court Technology Services Director for review and approval. The areas to be reviewed include, but are not limited to, physical security, access controls, system administration, operations security, change management, and disaster recovery/business continuity. Security controls established for each software layer (application, database, client/server operating system, and cloud-based system) must be identified. In addition, the confidentiality of the data must be addressed.

3.1.9 Software Testing

Software testing for systems that handle private, personal information must be accomplished with “sanitized” production information. Sanitized information is production information, which no longer contains specific details that might be valuable, critical, sensitive, or private.

3.1.10 Development Staff Access to Production Application Information

Development staff shall not have access to production data unless approved by the agency owning the data. In some cases, it may be necessary for software development staff to require long-term production access due to the services that have been requested of the development staff.

Control points must be identified to ensure that there are appropriate peer reviews. A staff developer that has written and tested code must not move that code to production until reviewed by another staff developer or Technology Services Director. At a minimum, separate directories or libraries with strictly enforced access controls must be employed.

Production access must be reviewed on an annual basis with the supported agency to ensure that access is still required.

3.1.11 Software Maintenance with Source Code

All permanent changes to production software must be made with source code rather than with object code or other executable code.

3.2 Change Control

3.2.1 Overview

All changes to software in use and/or added to the computing environment will follow the Kenton County Technology Services Department security standards for approval.

3.2.2 Software Changes/Configuration Management

The Kenton County Technology Services Department maintains an up-to-date inventory of computer software. Documentation records identify the name, version number, release date, platform, data owner, and domain/region of software residing on Kenton County computers. Existence of appropriate contractual agreements for use of vendor software is also documented.

3.3 Data Media/Security

3.3.1 Overview

All data and media must be sufficiently protected and monitored to prevent unauthorized use, modification, disclosure, or destruction. Security controls must be applied in a manner that is consistent with the value and classification of the data. Access to data must be granted to users only on a "need-to-know" basis, subject to approval by the designated data owner of the information assets.

3.3.2 Data Classification

All data must be appropriately reviewed to determine its level of sensitivity and/or criticality. If the environment has a mixed set of classified data, the classification that requires the most stringent controls must be used.

3.3.3 Storage & Transport

All media entering or leaving offices, processing areas, or storage facilities must be appropriately controlled. Storage areas and facilities for sensitive media shall be secured and all filing cabinets provided with locking devices appropriate to their sensitivity and protective requirements. Removable media must be stored in a fire-system protected receptacle or off-site storage facility.

Media containing sensitive information, such as PII or CJI should only be transported by authorized personnel, kept physically secure at all times, and encrypted wherever required per CJIS Security Policy, section 5.10.1.2.

Kenton County network users must not store sensitive information on workstation hard-disk drives. Note: workstation hard drives are NOT backed up by the Kenton County Technology Services Department. Any data lost as a result of a damaged workstation hard-disk drive is considered unrecoverable by the Kenton County Technology Services Department.

3.3.4 Disposal/Destruction

When a device used to access PII or CJI is disposed of or released for reuse to unauthorized individuals, the hard drive will sanitized in accordance with CJIS Security Policy Standards (Section 5.8.3), meaning overwritten at least three times or degaussed by, or in the presence of, CJIS authorized personnel.

If the device is slated for retirement, the hard drive will further be destroyed via either incineration or shredding, by, or in the presence of, authorized personnel. Formal documentation of all such hard drive

sanitization and destruction shall be maintained on file with the Kenton County Technology Services Department.

3.3.5 Electronic Transmission (E-mail, File Transfer Protocol, etc.)

If sensitive information is sent via the Internet or other unsecured media transmission facility, the information must be sent encrypted. Current encryption solutions include Virtual Private Networking (VPN), Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), secure FTP, and Secure Shell (SSH).

3.4 Internet Security

3.4.1 Overview

All data connections to external computer systems must be protected to ensure that only authorized users and data packets may connect with Kenton County computer systems. The level of filtering, supplemental authentication, audit logging, and associated access restrictions must be based on the risk posed by the computer systems and applications on both sides of the network connection.

3.4.2 Firewall

All connections between Kenton County Technology Services internal networks and the Internet (or any other publicly-accessible computer network) must pass thru the Kenton County firewall.

Only services that are explicitly authorized by the Kenton County Technology Services Director or the Kenton County Technology Services Network Engineer/Administrator will be permitted inbound and outbound between Kenton County internal computer networks and the Internet.

3.4.3 Exploiting Systems Security Vulnerabilities

Network users must not exploit vulnerabilities or deficiencies in information systems security to damage systems/information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted.

3.4.4 Cracking Passwords

Password cracking is defined as attempting to restore a lost or forgotten password through “brute-force” (repeatedly attempting to guess the correct password through systematic, automatic, or algorithmic password submission attempts) or by decrypting stored or saved passwords from their secure form. Password cracking is strictly prohibited.

3.4.5 Disabling Critical Components of Security Infrastructure

Critical components of the Kenton County Technology Services security architecture must not be disabled, bypassed, or turned off without prior approval from the Kenton County Technology Services Department Director. For example, critical components such as, but not limited to, firewalls, intrusion detection software, audit/event logging, must not be disabled without prior approval.

3.5 Workstation Security

3.5.1 Overview

All workstations shall have security policies to restrict unauthorized individuals and programs from accessing information and software stored in the workstation and associated peripherals.

3.5.2 Mandatory Protection for all Workstations

All workstations must have adequate controls to provide continued confidentiality, integrity, and availability of data. Critical business functions must not reside on workstations unless specifically authorized for that environment. All workstations must employ an approved access control mechanism to restrict access to authorized users. Network users must not leave their workstation unattended without first shutting down, logging out, or locking the workstation. The owner of the workstation has ultimate responsibility for the security of his/her workstation. Workstations must be configured to lock sessions after 30 minutes of inactivity, requiring a password to resume operation. Exceptions may be made for devices in a physically secure location or part of a criminal justice conveyance.

3.5.3 Protection for Sensitive Workstations

Workstation equipment must be physically protected to lessen the risks of theft, destruction, and unauthorized access to data.

3.5.4 Erasure of Restricted/Confidential Information

Sensitive data must be electronically erased from media or overwritten with approved software before the media leaves the Kenton County environment. This does not apply to confidential data written to media as part of scheduled backup processes. Due to the wide availability of programs to restore files that were accidentally deleted, the erasure of sensitive data must be accomplished by means other than deleting the file and as authorized by the Kenton County Technology Services Director.

3.5.5 Authorized Applications

Only Kenton County Technology Services authorized applications and utilities may be loaded on user workstations. Installing unauthorized applications can impact the performance of the workstation and potentially circumvent security controls. Unauthorized applications will be removed and the user will be subject to disciplinary actions up to and including termination.

3.6 Administrative Security

3.6.1 Overview

All operating systems, communications software, program products, security software, applications, and data must be sufficiently protected and monitored to prevent unauthorized use, modification, disclosure, or destruction.

3.6.2 Non Enforcement Does Not Imply Consent

Kenton County management's non-enforcement of any policy or procedure in this manual does not constitute consent. Kenton County management, at its discretion, may choose to enforce the provisions of this document at any time without prior notice. Kenton County network users should not expect that

out-of-compliance conditions are acceptable because management hasn't identified this activity in the past.

3.6.3 Access Control and Accountability

Login screens must include a special security notice. This notice must state: (1) the system may only be accessed by authorized users; (2) users who access the system beyond the warning page represent that they are authorized to do so; (3) unauthorized system usage or abuse may be subject to criminal prosecution; and (4) system usage may be monitored and logged.

The following subsections detail the access controls and accountability security policies.

3.6.4 Individual Access Authorization

Authorization for individual access must be based on a documented request (Employee Change of IT Access Form) that identifies resources required, and specifies access rights and privileges. The request must be submitted to the Kenton County Technology Services Director by the user's manager, who must educate the user on computing asset responsibilities. An Employee Change of IT Access Form is used to secure, terminate, transfer or otherwise change access to the network.

An Access Control List, providing a register of all network users and their permissions, must be actively maintained by the Network Engineer/Administrator and reviewed annually by Technology Services staff, managers, and relevant Agency heads as necessary to ensure all registered users are up to date.

3.7 User ID/Password Security

All users must have their identity verified with a User ID and password (or by other means which provide equal or greater security) prior to being permitted to use hardware or software connected to the Kenton County Network or to gain access to one of Kenton County's buildings protected by door access security.

3.7.1 Concurrent Connections

For applications accessing secure systems, fund accounting, or CJI, the number of concurrent connections must be set to one to prevent multiple people from sharing a User ID. Exceptions must include documentation of identified legitimate operational business needs requiring concurrent access.

3.7.2 Outsider User IDs

User IDs established for a non-employee/non-contractor must have a specified expiration date unless approved by the Kenton County Fiscal Court Technology Services Director.

3.7.3 Passwords

Passwords must be:

- Kept confidential;
- Changed whenever there is a chance that the password or the system could be compromised;
- Encrypted when held in storage or when transmitted across the network; and

Passwords must ***not*** be:

- Reused;
- Shared with other users;
- Repeated sequences of letters or numbers;

- Included in a macro or function key to automate the log-in;
- Stored in any file, program, command list, procedure, macro, or script where it is susceptible to disclosure or use by anyone other than the owner;
- Names of person, places, or things;
- The same as the User ID;
- Vendor default passwords (default passwords must be changed immediately upon use);
- Visible on a screen, hardcopy, or any other output device; and
- Hard coded into software developed (unless permission is obtained by the Kenton County Technology Services Director).

3.7.4 Password Composition

Password length must be eight (8) or more characters, use a combination of letters (upper/lower case) and numbers, and include at least one special character (any exceptions must be approved by Kenton County Technology Services Director).

3.7.5 Password History

Individuals must not reuse previously used passwords. To prevent this, a password history of 12 or more previous passwords must be kept.

3.7.6 Password Change

Network passwords must be changed by the user at least every 90 days (any exceptions must be approved by Kenton County Technology Services Director). If inadvertent disclosure is known or suspected, the passwords must be changed immediately.

3.7.7 System Process User Ids

System Process User IDs are application User IDs used to connect to a database.

The makeup of a non-expiring password is very important, as the strength of the password will determine how easily it can be broken. Every effort must be taken to ensure that the non-expiring password complies with the strictest interpretation of the password composition rules.

3.7.8 Assignment of Passwords

The initial password issued must be valid only for the user's first logon session. At that time, the user must be forced to choose another password before any other work can be done. The initial password must comply with password composition rules.

3.7.9 Minimum Password Age

Where supported, the minimum password age must be set to one day. This will help prevent users from "cycling" through passwords, thus bypassing the password history list. However, if inadvertent disclosure is known or suspected, the password must be changed immediately.

3.7.10 Storage of Administrative Passwords

Administrative passwords with special access must be stored in a file with password protection. Administrative passwords are communicated only to Kenton County Fiscal Court Technology Services staff with a need to know. The Director of Technology Services has the final say regarding who receives Administrative passwords and who does not receive them.

3.7.11 Password Generation Algorithms

Every effort must be taken to ensure that a generated password complies with the strictest interpretation of the KCFC password composition rules. If passwords or PINs are generated by a computer system, all software and files containing formulas, algorithms, and other specifics of the process must be controlled with the most stringent security measures supported by the involved computer system.

3.7.12 Personal Identification Numbers (PINs)

All PINs must be created with a similar construction as passwords in that they must not be numbers that are easily identifiable with the user. Password composition rules may not apply to PINs; however, other relevant password rules apply.

3.7.13 Cookies for Automatic Login

Web sites use cookies to store information on a computer. This information may contain personally identifiable information or log-in account information. Network users must refuse all offers by software to place a cookie on their computers so that they can automatically login the next time that they visit a particular Internet site.

3.7.14 Password and User ID Lockout

To prevent individuals from attempting to login with User IDs by guessing passwords, accounts will be locked after five (5) consecutive invalid login attempts for a minimum of ten minutes. Password resets must be requested by the user by contacting the Kenton County Fiscal Court Technology Services Department.

3.8 Networking Environment

This section describes practices specific to the Local Area Network Environment.

3.8.1 Access to Shared File Storage Areas (Directories)

The Kenton County Fiscal Court Technology Services Department recognizes that shared file directories are used to facilitate group work. It is a common business practice to use shared file directories. If shared files are restricted, access will be granted by authorization level. The following shared file directory authorization structure will be observed:

- The Kenton County Fiscal Court Technology Services Director and Network Administrator/Engineer will have the right to access all files.
- Agency leaders, Directors, Managers and Supervisors will have the right to access files under their area of supervision.
- An individual will have access to his or her individual files or other files as authorized by his or her Agency leader, Director, Manager or Supervisor.

3.8.2 Privileges

The least amount of security privileges required for a user to perform his or her job will be assigned.

3.9 Procedural Security

3.9.1 Overview

Kenton County agency leadership will procedurally monitor access and authorization to all sensitive information processed or stored in the computing environment.

3.9.2 Separation of Duties

Whenever computer-based processes involve sensitive, valuable, or critical information, the processes must include controls involving a separation of duties or other compensating control measures. These control measures ensure that no one individual has exclusive control over this type of information asset. To the extent possible, for every process involving sensitive, valuable, or critical information, at least two people are required to coordinate information-handling activities.

For example, application software in development must be kept separate from user acceptance test software, and production application software. In addition, access to user administration functions in critical software packages, such as financial management packages, must be controlled by resources other than employees of the finance office.

3.9.3 Individual Accountability

Individual User IDs will be assigned to people who access Kenton County computer networks. Depending on the individual's responsibilities, he or she may be assigned multiple User IDs on the same computer.

3.9.4 Output Distribution Controls

Confidential computer generated output must be personally delivered to the designated recipients and must not be delivered to an unattended desk, or left out in the open in an unoccupied office.

3.9.5 Audit Capabilities

Security software features must be used to automatically generate and store security audit log records for use in monitoring security-related events on all multi-user systems. The granularity and level of auditing should be commensurate with the sensitivity of the data.

3.9.6 Audited Events

For security systems, fund accounting systems, and any NCIC transaction handling systems, the following events shall be logged:

- Successful and unsuccessful system log-on attempts
- Successful and unsuccessful attempts to use:
    - access permission on a user account, file, directory or other system resource
    - create permission on a user account, file, directory or other system resource
    - write permission on a user account, file, directory or other system resource
    - delete permission on a user account, file, directory or other system resource
    - change permission on a user account, file, directory or other system resource
- Successful and unsuccessful attempts to change account passwords
- Successful and unsuccessful actions by privileged accounts (admin, DBA, etc)
- Successful and unsuccessful attempts for users to:
    - access the audit log file
    - modify the audit log file
    - destroy the audit log file

3.9.7 Audit Logs/Trails

To provide a logical audit trail, every audited event must be recorded with the following information:

- Date and time of occurrence
- Component of system where event occurred
- Type of event
- User ID

If there are instances where login activity cannot be recorded due to system constraints, notification shall be provided to the Kenton County Technology Services Director.

Audit logs are important for error correction, forensic auditing, security breach recovery, and related efforts. Audit logs must be secured such that they cannot be modified and can be read only by authorized persons.

All audit logs must be:

- Protected from unauthorized access, modification, or destruction;
- Reviewed at least weekly to confirm that there have been no attempted violations;
- Retained for a minimum of one (1) year.

To provide a physical audit trail, records of changes to the hardware and software inventory must be maintained.

Physical audit trail records must record:

- Identification of person maintaining or removing the computing asset;
- Date and time of maintenance event or removal;
- Identification of computing asset maintained or removed;
- Date and time when computing asset was returned;
- Inspection and acceptance of returned computing asset
- Date and time when computing asset was designated for surplus by Kenton County Fiscal Court

3.9.8 Security Violations

It is the responsibility of all Kenton County network users to report suspected security violations immediately to his or her supervisor who will then report to the Kenton County Fiscal Court Technology Services Director. A security incident is defined to be any event or threat of an event, affecting normal operation of a managed computer system and/or facility.

Security breaches may be categorized as those pertaining to physical intrusions and electronic intrusions.

3.9.9 Security Incident Reporting Procedure

The following procedure applies to incident reporting for all types of security breaches:

- Computing network users shall immediately report any suspected security breach to the Kenton County Fiscal Court Technology Services Director.
- An analysis of the findings and recommended actions will be documented as part of the investigation, including completion of the Security Incident Response Form (Appendix D)
- Configurations and/or procedures may be revised or developed as a result of the incident.
- The Kenton County Fiscal Court Technology Services Director will produce a summary report of the security incident.

Depending upon the nature of the incident, notification may also include the FBI, U.S. Attorney's Office, Kentucky State Police, Kenton County Police, Commonwealth Office of Technology and/or other law enforcement agencies.

For catastrophic disasters such as fire, bombs, floods, or destructive storms, notification procedures will include the Kenton County Emergency Management Department, and may include local fire department(s) and/or police department(s).

For incidents involving electronic intrusions, other county agencies will be notified as appropriate. Any data captured that results in detecting the intrusion will be kept until the incident has been investigated and cleared.

For incidents involving deception and fraud, additional notification may include the local police department(s) and/or the local County or Commonwealth Attorney's office depending upon the severity of the incident.

3.9.10 Security Incident Handling Procedure

The following procedure applies to incident handling for all types of security breaches.

- **Keep a Log**: Logging of pertinent information is critical in all situations. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log will be kept for security incidents that are under investigation.
- **Inform the Appropriate Personnel**: Informing the appropriate people is important. The Kenton County Fiscal Court Technology Services Director is responsible for notifying the Kenton County Administrator and appropriate executive level management of all reported incidents.
- **Release of Information**: Control of information during the course of a security incident or investigation is important. All release of information must be authorized by the Kenton County Administrator.
- **Follow up Analysis:** After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow up analysis will be performed. All involved parties will meet and discuss the actions that were taken and the lessons learned. All existing configurations and/or procedures will be evaluated and modified as needed.

Upon resolution of a confirmed security incident, Kenton County Technology Services will document the incident in detail with the Security Incident Reporting Form (Appendix D), a copy of which will be provided to the County Administrator, and kept on file.

3.9.11 Risk Management

The Kenton County Technology Services Director and the Network Engineer and Administrator are responsible for implementing security measures.

A formal review of the Kenton County computing and physical access environment will be conducted at least annually to ascertain the effectiveness of security control measures, identify weaknesses, recommend improvements to controls, and implement changes to strengthen areas where weaknesses are found. This includes documenting the validation of all system accounts.

3.9.12 Personnel Security

All members of the Kenton County Fiscal Court Technology Services Department will submit to a background check during the hiring process and additionally will submit to a National Crime Information Center (NCIC) background check. Prospective employees will be notified that a standard and NCIC background check will be performed as part of the recruiting and selection process.

3.9.13 Technology Policies and Procedures

Prior to new network users accessing Kenton County computer systems, their supervisor is required to ensure they are aware of the Kenton County's computer security policies. Directors, Managers and/or Supervisors must submit an Employee Change of IT Access Form for all new or departing employees. All new computing network users must sign the Technology Policies and Procedures document.

At least annually, all users of the Kenton County computing network will review and sign the Technology Policies and Procedures document as part of Kenton County's Technology Risk Management process.

3.9.14 Privacy

All messages sent over Kenton County computer and communications systems are the property of Kenton County. Kenton County reserves the right to examine all data stored in or transmitted by these systems. In accordance with the **Federal Electronic Communications Privacy Act of 1986**, employers can monitor electronic messages upon notification. Employees should have no expectation of privacy associated with the information they store in or send through these systems.

At any time and without prior notice, Kenton County management reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on Kenton County systems. This examination is performed to assure compliance with internal policies, support the performance of internal investigations, and to assist with the management of information systems.

Individuals may be subject to electronic monitoring while on Kenton County premises. This monitoring is used to measure to protect worker personal property, worker personal safety, and Kenton County property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

3.9.15 User Verification

When an individual requests his or her password be reset the Kenton County Fiscal Court Technology Services Director or staff designee must verify the identity of the requestor and ensure he or she has access to the User ID.

3.10 Internet and Email Use

Internet accessed via the Kenton County Network and e-mail addresses with a kentoncounty.org address are the property of Kenton County Fiscal Court.

3.10.1 Personal Use of Internet and Email

Incidental personal uses of Internet and E-mail resources are permissible, but not encouraged. Excessive personal use could lead to loss of the resource privileges and may result in disciplinary action up to and including dismissal. Staff members are responsible for exercising good judgment regarding incidental personal use. Any incidental personal use of Internet or E-mail resources must adhere to the following limitations:

- It must not cause any additional expense to the County or the staff members agency
- It must be infrequent and brief
- It must not have any negative impact on overall productivity
- It must not interfere with the normal business operations
- It must not compromise the agency or the County in any way
- It must be ethical and responsible

3.10.2 Implied Permission

The ability to connect with a specific Internet site does not in itself imply that a staff member is permitted to visit that site.

3.10.3 Expectation of Privacy

Staff shall have no expectation of privacy associated with E-mail transmissions and/or the information they publish, store, or access on the Internet using the County's resources.

3.10.4 Review of Employee Email or Internet Usage

If an employee is suspected of utilizing County internet or e-mail in an inappropriate or unapproved way, the Department Director should report this activity to the Director of Technology Services. Tools are in place to monitor staff member's use of e-mail and the Internet. The Network Engineer/Administrator shall review activity and email on the employee's behalf to determine if there is any cause for disciplinary action or review of policies with staff member.

3.10.5 Commercial Use

Agencies shall not accept commercial advertising or vendor-hosted website advertising for which the agency receives compensation. As a general practice, state agencies should avoid endorsing or promoting a specific product or company from agency websites, however the placement of acknowledgements, accessibility and certification logos are acceptable.

3.10.6 Prohibited and Unacceptable Uses

Unacceptable use of internet and email resources includes, but is not limited to the following:

- Downloading, installation or distribution of pirated software, digital music and video files.
- Using the Internet or E-mail for any illegal purposes, including communications that violate any laws, malicious use, spreading of viruses, and hacking.
- Using the Internet and E-mail for personal business activities in a commercial manner
- Procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, whether through language, frequency or size of messages.
- Knowingly accessing pornographic sites on the Internet and/or disseminating, soliciting or storing sexually oriented messages or images. The only exception to this is for law enforcement work necessitating its use.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or E-mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of E-mail.
- Forging E-mail headers to make it appear as though an E-mail came from someone else.
- Sending or forwarding chain letters or other pyramid schemes of any type.
- Sending or forwarding unsolicited commercial E-mail (spam) including jokes.
- Soliciting money for religious or political causes, advocating religious or political opinions and/or endorsing political candidates.
- Online investing, stock trading and auction services unless the activity is for County business.
- Use of peer-to-peer (referred to as P2P) networks.
- Any other non-business related activities that will cause congestion, disruption of networks or systems including, but not limited to, Internet games, online gaming, messaging services or similar Internet-based collaborative services.

Kenton County Technology Services reserves the right to restrict internet streaming services without notification to preserve bandwidth and protect network security.

3.11 Remote Work

3.11.1 Overview

Kenton County Technology Services offers a number of methods to enable employees to work from an external location. Requests for remote work capabilities for employees must be submitted by the Department Director to the Director of Technology Services, with approval of the County Administrator.

Department Directors should consider carefully the needs of their employees and the limitations of their job duties as to what can, and should, be allowed to be done remotely. Technology Services provides remote access that preserves the safety and security of information on the county network, but not any sensitive paperwork, such as tax forms or personnel information.

3.11.2 Phones

Employees can forward desk phone numbers to alternate phones using functionality in the desk phone itself. Technology Services personnel can also forward desk phones to alternate phones on employees' behalf.

3.11.3 Network Access

Specific permissions must be granted to an employee's user account by the Network Engineer/Administrator to enable access to the Kenton County network remotely. In order to preserve network security, this permission will not be granted unless requested by the Department Director and approved by the Director of Technology Services.

Additionally, employees will need to install the appropriate VPN client on their respective device in order to connect to the Kenton County Network. Employee must contact Technology Services with information about their device to receive instructions and assistance for the VPN client installation.

3.11.4 Workstation Access

Permissions must be granted to an employee's user account by the Network Engineer/Administrator to enable remote desktop functionality, allowing the user to access their work computer. In order to preserve network security, this permission will not be granted unless requested by the Department Director and approved by the Director of Technology Services.

3.11.5 Hardware Access

In order to utilize our VPN connection or Remote Desktop, users will need access to a device (laptop or desktop, tablet or other mobile device) and reliable internet connection. Kenton County Technology Services does not guarantee the provision of laptops for loan to departmental or agency employees.

Employees are expressly prohibited from removing hardware not designed for mobile work from the work site to use at home. Examples include monitors, keyboards, printers, and computer CPUs. Exceptions will only be made by direct permission from Technology Services Director.

3.11.6 Video Conferencing

Kenton County Technology Services provides limited support through different software packages for video conferencing. Workstation video cameras ("webcams") will only be provided if user has no mobile device with camera capability, or if user's job duties require the use of a workstation camera.

3.12 Physical Access Control

3.12.1 Overview

All Kenton County information processing areas must be protected by physical controls appropriate for the size and complexity of the operations and the criticality of the systems operated at those locations. Where necessary, additional physical security will be required, as outlined, for equipment used to access Criminal Justice Information (CJI) or Personally Identifying Information (PII).

The Kenton County Technology Services Department administers access security to Kenton County buildings with automated access control. It is the responsibility of each Director, Manager, or Supervisor to ensure that employees, contractors and visitors abide by these security measures. Each user's access through all secure doors or after hours is tracked and recorded for security purposes.

3.12.2 Building Access Keys

Building access keys, including keyfobs, keycards, or any other electronic access device, are issued to specific users and personnel and are prohibited from being shared with other users or personnel.

Upon departure of any employee, it is the responsibility of the Department Head to ensure that Technology Services is notified (Using an Employee Change of IT Access Form) so that the key can be permanently deactivated. Keyfobs and keycards are not to be reused by or reissued to a different employee.

If at any time a building access key is lost or stolen, it should be immediately reported to Technology Services, including the date and time the key was lost. It is the responsibility of Kenton County Fiscal Court Technology Services Department to verify there has been no unauthorized access from the lost key, in addition to deactivating the key and reissuing a new one to the user. In the event that a lost or stolen building access key is used for unauthorized access before deactivation, Technology Services will notify the user's supervisor to determine the severity of the breach, and consult building maintenance and the Director of Homeland Security & Emergency Management if needed.

Department Heads may request a report on access into their restricted areas, or the activity of their staff throughout all access control points, including times and dates of entry.

3.12.3 Hardware Security

Adequate security measures must be in place to protect Kenton County computer and communications equipment and data from physical damage, theft, or vandalism. To satisfy this requirement, the following must be maintained:

Inventory: A current record of the physical computing assets or group of assets.

Rooms to Protect Equipment: Rooms intended to secure hardware must provide for:

- Limited physical access; and
- Protection against environmental hazards.

Workstation and Terminal Control: Devices outside computer or communications rooms must be:

- Logged off or physically secured when unattended;
- Housed in a facility that provides adequate protection from theft; and
- Protected from environmental hazards.

Portable Equipment Control: An employee who receives permission to remove equipment from a Kenton County site must provide a reasonable level of protection for that equipment and associated

software, data, and media from theft and damage. A record of portable equipment assigned to employees must be maintained by the individual or group authorized to distribute the equipment.

3.12.4 Hardware Changes/Configuration Management

All computer and communications systems must employ a formal change control procedure to ensure that only authorized changes are made. The change control procedure must be used to document all significant changes to software, hardware, communications links, and operational procedures.

3.12.5 Theft Protection

To minimize the risk of theft adequate deterrents such as locked rooms and storage areas, controlled access rooms, and monitoring of visitors is performed. Employees issued laptops or tablets cannot check these computers into airline luggage systems.

Whenever sensitive information and/or equipment is removed from Kenton County premises, a record of the date, the information/equipment involved, and the persons possessing the information/equipment will be made. If the equipment contains sensitive information additional safeguards such as encrypting the data must be employed.

3.13 Disaster Recovery and Backup

3.13.1 Overview

An integral component of effective contingency planning is the regular backing up and storing off-site of all critical applications, software, documentation, and data files. The Kenton County Fiscal Court Technology Services Department will maintain an effective schedule for the backup of critical computer and network resources and for the prompt recovery of services following unanticipated interruptions. This schedule will include On-site backups, Off-site regionally accessible backups, and Off-site outside of region accessible backups.

3.13.2 Data Backup

On-site backup is used to have current data readily available in the event operating data is lost, damaged, or corrupted. Off-site backup embodies the same principle but provides an additional protection against threats potentially damaging to the primary site and data. Off-site out of region backups provide a last resort protection against regional natural disasters or other site specific issues preventing access of previous forms of backup.

All systems shall be reviewed regularly by the Technology Services Director and Network Engineer/Administrator to identify the best backup method for each system, including backup method, frequency of backups taken, duration of time backups are retained, and where they are stored. This information shall be documented and updated as needed.

4. Appendix A – Mobile Device Use Policy

4.1 Policy Statement

Kenton County recognizes that the performance of certain job responsibilities may be enhanced by or require the use of a mobile device, including cellular (cell) phones, tablets, and portable internet connection devices ("hotspots" or "MiFis"). This policy applies to all Kenton County Fiscal Court employees who are issued a mobile device, or an employee of any associated agency provided one of these devices by Kenton County Fiscal Court.

4.2 Eligibility

An employee is eligible for a County-owned cell phone if at least one of the following criteria is met:

- The job function of the employee requires considerable time outside of his/her assigned office or work area and it is important to the County that s/he is accessible during those times;
- The job function of the employee requires him/her to be accessible outside of scheduled or normal working hours where time sensitive decisions/notifications are required;
- The job function of the employee requires him/her to have wireless data and internet access.

An employee who only occasionally is contacted for business purposes is not eligible for a County-owned mobile device.

4.3 Equipment Purchase of Employee Mobile Devices

The County will not pay for the purchase of personal cell phones, tablets, MiFis, activation fees, monthly service fees, or insurance for employees.

4.4 Oversight, Approval, and Funding

Department Directors are responsible for identifying employees who hold positions that include the need for a mobile device. Each department is encouraged to review whether a wireless device is necessary, and to select alternative means of communication when such alternatives would provide adequate and less costly service to the County.

Annually, the need for a mobile device will be reviewed by each Department Director, with the assistance of the Technology Services Director, to determine if existing issued phones should be continued, changed, or discontinued. The County Administrator reviews Department Director recommendations and has final approval authority of Department Director recommendations. Exceptions to any of these policies must be approved by County Administrator.

County-owned mobile devices are funded by the department submitting the request. Employees are not permitted to supplement the cost in order to facilitate a device purchase or upgrade beyond the scope of what the Department Director deems appropriate. Employees may request permission from Department Director and Technology Services Director to use personally owned mobile devices on the County wireless account, provided all of the following:

- Employee has already been approved to receive a county-owned mobile device
- Use of employee's personally owned device poses no additional costs to County
- Employee accepts full responsibility for maintenance of personally owned mobile device
- Employee acknowledges that personally owned devices are not exempt from Open Records Requests

4.5 Use of Personal Mobile Devices

The County is not responsible for the purchase of, service for, or payments on any personal use mobile device. The County does not accept any liability for claims, charges or disputes between the service provider and the employee. The County does not provide service or support for personally owned mobile devices, with the following exceptions.

Support from the County's Information Technology Department is limited to connecting a personally-owned smartphone or tablet to County-provided services, including email, calendar, and contacts. Any mobile device connected to these services that has data capabilities must be secured based on current County determined security standards including password protection and encryption, regardless of whether it is a personal device or county-owned.

Employees are expected to delete all County data from the mobile device when their employment with the County is severed, except when required to maintain that data in compliance with a litigation hold notice.

4.6 County Owned Mobile devices

The County may own and issue mobile devices for emergency, disaster recovery, and/or other business purposes, including:

- Public Safety
- On-call department(s) cell phone(s)
- Supervision cell phone(s) used by supervisors throughout the day and who may be subject to calls in the off times.
- Tablets for enabling work outside of the office
- Mobile hot spot to allow employee to access wireless internet on mobile devices or laptops for work purposes.

If a mobile device is stolen or missing, it must be reported to the employee's supervisor, the wireless device service provider, and to the County's Technology Services Department as soon as possible.

The County is responsible for purchasing its mobile devices and establishing a service contract with a cell phone service provider of its choice. The cell phone contract is in the name of Kenton County Fiscal Court, who is solely responsible for all payments to the service provider.

Employees are expected to return County-owned mobile devices to the County's Technology Services Department when their employment with the County is severed. All County data should be deleted from the mobile device when their employment with the County is severed, except when required to maintain that data in compliance with a litigation hold notice.

Data stored on a county-owned mobile device, including documents, communication, pictures, and apps are considered the property of Kenton County Fiscal Court, and may be subject to Open Records Requests or review by a Supervisor.

4.7 Cancellation

Any County-owned mobile device will be immediately cancelled or suspended if:

- The employee terminates employment with the County.
- The employee changes position within the County which no longer requires the use of a mobile device for business reasons.
- There is misuse/misconduct with the mobile device.
- A decision by management (unrelated to employee misconduct) results in the need to end the program or there is a change in the employee's duties.

4.8 Use while operating machinery

County staff are prohibited from text messaging while driving county-owned vehicles or during work hours. Mobile Devices are only approved for use while operating machinery when designed specifically for that business purpose and approved by both Department Director and Director of Technology Services.

5. Appendix B – Protection of Personal Information: Security and Breach Investigation Procedures & Practices

This Policy is adopted pursuant to KRS 61.931-61.934 and Department for Local Government Policy Number DLG-PPI 100.

5.1 Introduction

5.1.1 Definitions

- "County" means Kenton County.
- "Computer security incident" or "incident" means a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- "COT" means the Commonwealth Office of Technology.
- "Digital media" means physical, electronic media, used to store information, including, but not limited to: diskettes, magnetic tapes, desktop computers, laptops, hard drives, random access memory, read only memory, compact discs, network equipment, other forms of optical and magnetic media, and any other electronic media on which information may be stored. This definition includes forms of media existing at the time these regulations are promulgated and also any such forms or formats as may be invented.
- "DLG" means the Department for Local Government.
- "Non-digital media" means a hard copy or physical representation of information, including, but not limited to, paper copies, printer ribbons, drums, microfilm, platens, and other forms of preserved or preservable information.
- "Personal Information" means an individual's first name or first initial and last name or personal mark, in combination with one (1) or more of the following data elements:
    - An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
    - A Social Security number or taxpayer identification number that incorporates a Social Security number;
    - A driver's license number, state identification card number, or other individual identification number issued by any agency;
    - A passport number or other identification number issued by the United States government; or
    - Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;
- "Point of Contact" or "POC" means the designated Point of Contact with respect to this Policy.
- "Portable computing device" means electronic devices on which personal information is stored, or may be stored, designed, used or intended to be used in multiple physical locations or capable of being used while traveling, such as laptops, tablet computers, iPads, cell phones, digital cameras, and similar devices.
- For purposes of this policy, all terms not otherwise defined are used consistent with the definitions set forth in KRS 61.931.

5.1.2 Policy Statement

This Policy is based on DLG Policy Number DLG-PPI 100 and is intended to minimize the risk of the County disclosing personal information and setting practical guidelines for effectively responding to security incidents.

This Policy sets forth the procedures and practices pursuant to KRS 61.932 for the County to follow in order to:

- Identify vulnerabilities;
- Eliminate or mitigate those vulnerabilities;
- Recognize when an incident has occurred;
- Notify appropriate personnel in the event of an incident;
- Respond to information security threats; and
- Recognize events that require special handling due to their potential impact or special reporting due to legal or other concerns.

In addition, this Policy requires the County to enact appropriate measures to protect information stored on media, both digital and non-digital, during the entire term of its use, until its destruction.

5.1.3 Applicability

This Policy shall be followed by the County and by any and all persons or entities with access to personal information in the possession or control of the County. Such persons or entities include, but are not limited to, employees, contractors, consultants, temporary employees, volunteers and other workers with access to personal information whether printed, electronic or other format.

5.1.4 Responsibility for Compliance

The County shall ensure that employees and others with permissive access to, or who may access, personal information are familiar with this Policy and all such persons or entities shall be aware of what constitutes an incident. The County shall ensure that employees are aware that compliance with this Policy is mandatory. The County shall have the responsibility to enforce this Policy.

5.2 Policy

Non-digital media containing personal information shall be physically controlled and securely stored in a manner meant to ensure that the media cannot be accessed by unauthorized individuals. This may require storing media in locked containers such as cabinets, drawers, rooms, or similar locations if unauthorized individuals have unescorted access to areas where personal information is stored. If personal information is stored in an electronic format, it shall be protected from access by unauthorized individuals. Such information must be protected by software that prevents unauthorized access. If personal information is transmitted via e-mail or other electronic means, it must be sent using appropriate encryption mechanisms.

5.3 Procedures

5.3.1 Point of Contact

The Technology Services Director is hereby designated as Point of Contact ("POC") with respect to this Policy. The POC shall serve the following functions:

- Maintain the County's Policy and be familiar with its requirements;
- Ensure the County's employees and others with access to personal information are aware of and understand this Policy;
- Serve as contact for inquiries from other agencies regarding this Policy and any incidents;
- Be responsible for ensuring compliance with this Policy; and
- Be responsible for responding to any incidents.

5.3.2 Software

Security software used to protect personal information must provide user identification, authentication, data access controls, integrity, and audit controls.

Security software should be adequately tested to confirm functionality and to ensure that it is minimally disruptive to all associated operating systems, communications, applications, and other associated software systems. Contractual provisions must also ensure that the supplier's software, by design or configuration, will not introduce any security exposures.

The level of protection afforded by security software should be commensurate with the sensitivity of the data. For example, if data resides in a database that is deemed highly confidential, stringent access controls to the database should be employed. The level of protection along with the methods to implement that protection should be addressed before any personal information is stored on a device.

Systems, networks and application software used to process personal information must adhere to the highest level of protection reasonably practical. The County shall use Intrusion Detection and Prevention software approved by COT. A list of approved software is available on the COT website. As an alternative, the County may use software not approved by COT, provided that such software provides comparable, or superior, protection.

5.3.3 Encryption

Information stored on digital media shall be encrypted in accordance with contemporary standards.

5.3.4 Access Control

Only authorized individuals are permitted access to media containing personal information. In addition to controlling physical access, user authentication should provide audit access information. Any access must comply with applicable regulatory requirements.

5.3.5 Portable Computing Devices

This Policy prohibits the unnecessary placement (download or input) of personal information on portable computing devices. However, users who in the course of County business must place personal information on portable computing devices must be made aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of personal information. If

personal information is placed on a portable computing device, reasonable efforts must be taken, including physical controls and encryption, to protect the information from unauthorized access. Additionally, each person using the portable computing device must sign a form approved by the County indicating acceptance of the information and acknowledging his/her understanding of the responsibility to protect the information. In the event the portable computing device is lost or stolen, the County should be able to accurately recreate the personal information and must be able to provide notification to all affected persons/entities.

When it is determined that personal information must be placed on a portable computing device, every effort should be taken to minimize the amount of information required. If possible, information should be abbreviated to limit exposure (e.g., last 4 digits of the social security number).

5.3.6 Physical Security Procedures

The POC shall adopt and implement physical security procedures consistent with this Policy. When feasible, information technology equipment should be marked with some form of identification that clearly indicates it is the property of the County. During transport, media shall be protected and controlled outside of secured areas and activities associated with transport of such media restricted to authorized personnel. Tracking methods shall be developed and deployed to ensure media reaches its intended destination.

5.4 Protection of Personal Information

The County shall secure and, when applicable, appropriately dispose of non-digital media. Non-digital media containing personal information must be properly stored and secured from view by unauthorized persons.

Secure measures must be employed by the County and all permissive users to safeguard personal information contained on all County technology resources.

The County shall ensure that all authorized personnel are familiar with and comply with this Policy. The County shall ensure that only authorized personnel may hold and have access to personal information.

5.5 Types of Incidents

Threats to the security of personal information arise in many different ways. Persons covered by this Policy are encouraged to be aware of the different types of threats and to enact reasonable measures to protect against each. Attacks on personal information may arise from:

- External/Removable Media—an attack executed from removable media (e.g. flash drive, CD) or a peripheral device.
- Attrition—an attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
- Web—an attack executed from a website or web-based application.
- Email—an attack executed via an email message or attachment.
- Improper usage—any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- Loss or Theft of Equipment—the loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- Other—an attack that does not fit into any of the other categories.

5.6 Destruction of Records Containing Personal Information

The County shall retain and destroy records consistent with applicable Records Retention Schedules established by the Kentucky Department of Libraries and Archives and its own document/information retention policy.

When records containing personal or confidential information are ready for destruction, the County shall destroy the information completely to ensure that the information cannot be recognized or reconstructed. In addition, any personal or confidential data contained on the computer media must be obliterated and/or made indecipherable before disposing of the hard drive, tape, diskette, CD, USB drive, or other type of medium.

The POC shall provide appropriate methods and equipment to routinely destroy personal or confidential information. The methods set forth below are listed in the priority order established by DLG with the most highly recommended safeguard listed first. One of the following safeguards must be implemented:

- Hire a document disposal contractor to dispose of the material. The contractor should be certified by a recognized trade association and should use disk sanitizing software and/or equipment approved by the United States Department of Defense. The County should review and evaluate the disposal company's information security policies and procedures. The County should review an independent audit of a disposal company's operations and/or its compliance with nationally recognized standards.
- Secure and utilize shredding equipment that performs cross-cut or confetti patterns.
- Secure and utilize disk sanitizing or erasing software or equipment approved by the United States Department of Defense.
- Modify the information to make it unreadable, unusable or indecipherable through any means.

5.7 Reporting of Incidents Involving Personal Information

The County must disclose a security breach in which personal information is disclosed to, or obtained by, an unauthorized person. Notification of the incident must be made in the most prompt and expedient manner after the incident has been discovered. Within thirty-five days, a letter notifying affected individuals of actual or suspected loss or disclosure of personal information must be sent by the County describing the types of information lost and recommended actions to be taken to mitigate the potential misuse of their information.

When the County identifies that a security breach has occurred in which personal information has been disclosed to, or obtained by, an unauthorized person, within three business days it shall notify Kentucky State Police, the Auditor of Public Accounts, the Attorney General and the Commissioner of the Department for Local Government and complete form COT-F012. The County shall document the following:

- Preliminary Reporting and description of the incident;
- Response, including evidence gathered;
- Final Assessment and corrective action taken; and
- Final Reporting.

Incident Response procedures can be a reaction to security activities such as:

- Unauthorized access to Personnel, Data, or Resources;

- Denial of Service Attacks;
- Actual or Anticipated Widespread Malware Infections;
- Data Breaches;
- Loss/Theft of Equipment;
- Significant Disruption of Services;
- Significant Level of Unauthorized Scanning Activity to or from Hosts on the Network.

5.8 Investigation and Disclosure

5.8.1 Investigation

The County shall make reasonable efforts to investigate any security breaches in which personal information is disclosed to, or obtained by, an unauthorized person and shall take appropriate corrective action.

5.8.2 Disclosure Communications

The County must comply with all federal and state laws and policies for information disclosure to media or the public. In some circumstances, communication about an incident is necessary, such as contacting law enforcement.

The County should use discretion in disclosing information about an incident. Such information includes network information, type of incident, specific infection type (if applicable), number of assets affected, specific detail about applications affected, applications used to employ corrective action/investigate, etc.

The County may proactively share relevant incident indicator information with peers to improve detection and analysis of incidents. Within the parameters of the law, minimal disclosure regarding incidents is preferred to prevent unauthorized persons from acquiring sensitive information regarding the incident, security protocols and similar matters, in an effort to avoid additional disruption and financial loss.

6. Appendix C – Social Media Use Policy

6.1 Summary

Kenton County uses social media as a way to communicate with stakeholders, media, employees and residents, and to promote the County, County services, job opportunities and County events. This policy outlines how Kenton County will use social media and will continually evolve as new technologies emerge. Kenton County's social media policy applies to all personnel that fall under the leadership of the County Administrator including volunteers, vendors and contractors.

6.2 Definitions

6.2.1 Social Media Sites

External websites or services on non-county servers. Most social network services provide a variety of ways for people to interact, such as e-mail and instant messaging services.

6.2.2 Content Manager

Individual responsible for maintaining all information on a Social Media Site. Kenton County's appointed Content Manager is the Communications Coordinator, acting under the direction of the Judge/Executive, County Administrator and Department Directors.

6.2.3 Posting

The publishing of information on Social Media Sites.

6.2.4 Blogs

Any type of website with regular entries of commentary, descriptions of events, or other material such as graphics or video.

6.2.5 Social Networking

The use of a variety of websites that allow users to share content, interact, and develop communities around similar interests.

6.3 Selection of Social Media Sites

6.3.1 Authority to Create Sites

The Communications Coordinator will review a site before a County account is created. Accounts will be created based on need, purpose and audience. County accounts shall only be established by the Communications Coordinator.

- County Department Director social media accounts in which the account represents the County Department Director in his/her official role, must be approved by the Communications Coordinator and must conform to 6.4 Use of Social Media Sites guidelines outlined in this policy and must complete a Social Media Authorization Form.
- Postings regarding official County business may be subject to the Kentucky Public Records Act (KRS 61.870-61.884) and the Open Meetings of Public Agencies Act (KRS 61.800-61.850).
- County Elected Officials must also be aware that postings regarding official County business may be subject to the Kentucky Public Records Act (KRS 61.870-61.884) and the Open

Meetings of Public Agencies Act (KRS 61.800-61.850). It is advised that Elected Officials consult the Communications Coordinator regarding postings.

6.3.2 Social Media Tools

Social media tools include, but are not limited to:

- Team and group sites such as Google Sites, SharePoint, Yahoo Groups
- Blogs such as WordPress
- Micro-blogs such as Twitter
- Social networking sites such as Facebook and LinkedIn
- Visual media sharing such as YouTube, Flickr or Instagram

6.3.3 Communications Coordinator Responsibilities

The Communications Coordinator shall be responsible for the following:

- Reviewing concept, audience, marketing plan, and content strategy for any Social Media Site.
- Collaborating any external web applications with the Technology Services Department to ensure it is technically compatible with the County's network environment and browsers.
- Setting up the main administration account for the site, using a County e-mail address.
- Determining whether the site allows comments or posts to be turned off. It will be at the discretion of the County Administrator whether a site or platform will be used in the event that the particular format will not allow the County to turn off the comments or posts feature.
- Oversee and confirm decisions regarding social media sites including authorization of sites and additional page users
- Evaluate requests for usage of social media accounts & channels
- Verify staff authorized to use social media tools
- Maintain a list of social media domains, active account logins and passwords
- Change passwords if employee is removed as administrator
- Review the Social Media Sites on a routine basis to ensure they are updated and that information is being posted in a timely manner.
- Review all County-related information prior to posting on Social Media Sites, unless it contains time sensitive information that is being posted by an approved additional user, as outlined under 6.4 Use of Social Media Sites.

6.4 Use of Social Media Sites

6.4.1 Site Compliance

County use of social media sites will comply with all provisions of Kentucky law, ordinances of Kenton County, and policies issued by the County Administrator.

6.4.2 Administration of Social Media Sites

All County social media sites shall clearly indicate that they are maintained by the County and shall have Kenton County contact information available on the site. All County social media sites and services shall be registered and administered through the Kenton County Fiscal Court Technology Services Department.

6.4.3 Departmental Social Media Accounts

Individual County departments and individual staff members may not establish their own official Kenton County Social Media Sites/Pages. Individual departments wanting to add content to official County Social Media Sites may submit requests to the Communications Coordinator for approval.

A Department Director may designate an employee to work with the Communications Coordinator, pending approval, to administer the departmental social media site and serve as an author and/or moderator for postings.

- The Communications Coordinator may approve an additional user, designated by the Department Director, to manage and post on an approved social media account. This user, designated by the Department Director and approved by the Communications Coordinator, will be trained and must complete a Social Media Authorization Form.
- This additional user should send information to be posted to the Communications Coordinator prior to posting, unless the Communications Coordinator is unavailable and the content contains time sensitive information that adheres to the guidelines set forth by the County.
- All employees who have access to County Social Media Accounts must lock their computer while away or log off the site to ensure security of the accounts.
- If an employee accesses County Social Media Accounts from a mobile device, the employee must have a passcode to access applications on the mobile device.
- All employees who have access to County Social Media Accounts must establish two-factor authentication on platforms where this is available for security purposes.

6.4.4 Website

Kenton County's website, http://www.KentonCounty.org, will remain the official location for content regarding official County business, services and events. When possible, links within Social Media formats will direct users back the County's website for more information, forms, documents or online services necessary to conduct business with Kenton County.

6.4.5 Hours of Moderation

Kenton County Social Media channels will be monitored Monday-Friday 8:00 A.M. to 5:00 P.M. except on County approved holidays.

6.4.6 Comments

If a social media site or any other internet based platform used by the County allows for comments to be posted by the public, the Communications Coordinator reserves the right to edit or remove the comments based on the Terms of Use criteria, and for any other appropriate reason.

The County also reserves the right to turn off the ability of third parties to post or comment.

The County's intent is not to create a public forum, but to maintain a moderated online discussion on a Limited Public Forum directly relating to topics posted by the County, with language that is appropriate for all residents, (including minors) to read.

6.4.7 Terms of Use Policy

The following Terms of Use policy will be available on social networking accounts, adapted to the appropriate department:

This is the official Facebook page for Kenton County, Kentucky. Kenton County encourages posts and comments. Prior to posting comments on this Limited Public Forum, users must review and agree to the Terms of Service of Facebook and also the Terms of Use of the Kenton County Facebook page. A submitted comment or posting on this page shall constitute an acknowledgement and agreement of these Terms of Use. All posted content (comments, photos, links, etc.) must be related to the topic at hand. Posts and comments that fall into the following categories are prohibited:

- *not topically relevant*
- *promoting or advertising commercial services, entities, or products;*

- *supporting or opposing political candidates or ballot propositions;*
- *obscene;*
- *personal attacks;*
- *name calling;*
- *infringements on copyrights or trademarks;*
- *illegal activity or encouragement of illegal activity;*
- *promoting, fostering, or perpetuating discrimination on the basis of creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, or sexual orientation;*
- *information that may tend to compromise the safety or security of the public or public systems;*
- *content that violates a legal ownership interest of any other party;*
- *anonymous*

Kenton County reserves the right to remove posts or comments that do not comply with this policy. All posts and comments uploaded to the Kenton County Facebook page will be reviewed periodically. Kenton County is not responsible for any postings or comments deemed inappropriate that cannot be removed in a timely fashion. All posts and comments are public records subject to public disclosure under the Public Records Act (KRS 61.870-61.884).

The posts and comments on this site do not necessarily reflect the opinions or positions of Kenton County or its employees. If you have questions or problems concerning the operation of this site, please contact Kenton County's Communications Coordinator.

6.4.8 Disabling of Functions

The Communications Coordinator may disable functions on the Social Media Site or applications that are not needed or desired in the sole discretion of the County. No rights are created in any third party with respect to how the County may utilize the applications and features on social media or web application sites, and the decisions on which features to maintain or disable will be in the sole discretion of the County.

Similarly, the decision to allow posting or responses by third parties and the removal of any such responses or postings shall be the sole discretion of the County and outside parties do not have any authority or right to control content or the length of time content may be posted.

Kenton County reserves the right to temporarily or permanently suspend a channel, or permanently suspend posting access to official County Social Media Sites at any time.

6.4.9 Personal E-mail Addresses

No County employee personal e-mail addresses should be posted on these sites.

6.4.10 Public Records Act Compliance

All information posted by the County on external sites may be subject to the Kentucky Public Kentucky Public Records Act (KRS 61.870-61.884) and the Open Meetings of Public Agencies Act (KRS 61.800-61.850).

6.4.11 Public Requests & Questions

County social media established pursuant to this policy will not be appropriate places where a person may request public records. County social media will not be monitored for public records requests. The County staff responsible for implementation of this Policy and for providing services on behalf of the County with respect to social media, are not custodians of general public records. Requests for public records should be directed to the Assistant County Administrator.

County social media will not generally be an appropriate forum by which residents may ask questions or request information or records of the County. Residents are requested to go to the official County website at http://www.KentonCounty.org and link to the place established on that website for general inquiries directed to the County. Questions that may be posted on County social media may not receive an answer because the site will not be monitored for this purpose. Questions answered by County staff on social media do not imply a change to this policy.

7. Appendix D – Security Incident Response Form

7.1 Security Incident Reporting Form

Name of Person Reporting Incident:				
Date of Report:		**Date of Incident:**		
Point(s) of Contact:	**Name (First & Last)**	**Title/Role**	**Phone**	**Email**
Location(s) of Incident:				
Incident Description:				
System(s) Affected:				
Method of Detection:				
Actions Taken/ Resolution (See 7.2 below for examples)				

Copies of this completed form shall be provided to Kenton County Administrator and all impacted agencies/departments to be kept on file.

7.2 Post-Incident Activity

Post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?