

RESOLUTION – 16-11
MADISON COUNTY FISCAL COURT

**A RESOLUTION ADOPTING AND APPROVING THE MADISON COUNTY
DEPARTMENT OF INFORMATION TECHNOLOGY POLICIES AND PROCEDURES**

Whereas, the Madison County Fiscal Court desires to implement policies and procedures to ensure the protection of Madison County, KY Information Assets from accidental or intentional unauthorized access; and

Whereas, these five policies are specifically have protocols established by the Madison County Fiscal Court and by the State of Kentucky. The policies pertain to Information Security(IT-01.100), User ID and Passwords(IT-02.100), Media Sanitization(IT-03.100), Clean Desk Policy(IT-04.100), and Access Channel 46(IT-06.100); and

Whereas, the five policies are noted as attachments to this resolution and are numbered as noted in the above paragraph.

Now therefore, be it resolved by the Fiscal Court, the attached documents be adopted by this Fiscal Court the 13th day of September, 2016.

SIGNED

R, EJ -
Reagan Taylor
County Judge Executive

ATTESTED

Kenny Barger
Kenny Barger
County Clerk

Department of Information Technology
Madison County, Kentucky

Policy Number: IT-01.100

Effective Date: 10/10/2016
Revision Date: 09/08/2016
Next Review Date: 07/01/2018

Subject: Information Security Policy

Applicability: This policy is applicable to all Madison County Fiscal Court Employees, nonaffiliated third party or anyone granted use of a Madison County Fiscal Court Information Asset. Every user of any of Madison County, KY Information Assets has a level of responsibility toward the protection of those assets. This policy refers to all Madison County, KY Information Assets whether individually-controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated or contracted to a nonaffiliated third party by Madison County, KY. This includes networking devices, laptops, tablets, telephones, smart phones, wireless devices, personal computers, virtual desktops, workstations, servers, minicomputers and any associated peripherals and software, regardless of their individual purpose.

Maintenance: The Department of Information Technology has the responsibility for the maintenance of this policy. This policy will be reviewed at least every two years.

Responsibility: Departments, agencies and all staff outlined in the Applicability section are required to understand and follow the guidelines set forth in this document. Each department or agency is responsible for assuring that their staff have been made aware of the provisions and that compliance is expected. Departments, agencies and staff shall also be aware that the intentional, inappropriate use may result in disciplinary action up to and including termination. Agencies that fail to comply may result in service charges to the agency for Madison County Fiscal Courts efforts to remedy the actions resulting from inappropriate Information Security Operations.

Purpose: The purpose of this policy is to ensure the protection of the Madison County, KY Information Assets from accidental or intentional unauthorized access. This policy establishes Madison County, KY strategy and its responsibilities for ensuring the Confidentiality, Integrity and Availability of Information Assets that are owned or operated by Madison County, KY. Information assets addressed by this policy include the following: data, information, information systems, computers/servers, network devices and any information regardless of its medium or regardless of its location.

By implementing an Information Security Policy, Madison County, KY will:

Establish an information security framework to appropriately safeguard access to information resources and services; Protect against unauthorized access to use or share restricted digital assets that could potentially result in harm to Madison County, KY, to Madison County, KY Employees or Citizens of the community; Safeguard against anticipated threats or hazards to the security of information assets; Comply with federal, state and local law.

Policy: Employees, nonaffiliated third parties and anyone else that have been granted use of a Madison County, KY Information Asset have a shared responsibility to protect the information assets that are owned and operated by Madison County, KY.

1. Data & Systems Protection

- 1.1. **User ID – Password Protection:** The Information Technology Department will authorize all access to Madison County, KY Information Assets. Each user is responsible for establishing and maintaining a password that complies with Madison County, KY **Password Policy (IT-02.100)** for each system as required. The use of another user's account or attempt to capture other users' passwords is prohibited. Each user is responsible for restricting unauthorized access to the Information Assets by locking their computer or logging out of their computer account when leaving their computer unattended. Staff who discover unauthorized use of their accounts must immediately report it to the Information Technology Department.
- 1.2. **Encryption:** Encryption Methods used must meet or exceed the adopted standards set forth by the Nation Institute of Standards Technology (NIST) as part of the Federal Information Processing Standards (FIPS) and renders the data indecipherable without the associated cryptographic key to decipher the data. The Current Standard is NIST 800-175B, FIPS 140-2.
- 1.3. **Data Protection:** Madison County, KY will take the necessary steps to protect the confidentiality, integrity, and availability of all of its Information Assets. Madison County, KY defines its data classifications as listed below
 - 1.3.1. **Critical/Sensitive Data** is of the highest priority which is defined as information which if released could damage Madison County, KY financially; put staff or citizens at risk; put facilities at risk; or could cause legal liability as defined as Personal health information, social security numbers, credit card holder information, bank information, police investigation information or personal information.
 - 1.3.2. **Personal Information** is defined as any individual's first or first initial and last name; personal mark or biometric image in combination with one or more of the following data elements; Any Account Number, Credit/Debit Card number in combination with any security code or password that would permit access to an account, Social Security Number, Taxpayer identification number that incorporates a Social Security Number, Driver's License number, state identification number or any other individual identification number issued by an agency, Passport Number or other identification number issued by the United States Government, Individually identifiable health information as defined in 45 C.F.R sec. 160.103
 - 1.3.3. **General Use Information** is defined as all other data stored on a Madison County, KY information asset that does not warrant specific protection but shall be protected appropriate to its use. Madison County, KY will restrict access to any and all data to only individuals that have a legitimate business need-to-know.
 - 1.3.4. **Critical/Sensitive Data Form** – Each Department or Agency is required to fill out a **Critical/Sensitive Data Form (IT-F1004)** that will define data that is stored on the Madison County, KY network that is deemed Critical/Sensitive Data
 - 1.3.5. **Responsibility of Protection:** All Individuals with access to any data are responsible for its protection. Individuals with access to critical/sensitive information must take reasonable steps to ensure the safety of

critical information including: not putting critical/sensitive data on unencrypted laptops or USB drives; that data is encrypted any time it is electronically transported outside the Madison County network; not storing, saving, or transmitting critical/sensitive data to a home computer or other external computer; ensuring inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it. Critical/sensitive data shall not be transported on unencrypted devices such as thumb drives, CD/DVD's or smart phone devices. Information Technology approval is required prior to moving any and all devices containing information that is considered critical/sensitive. These request should be made in advance.

- 1.4. **System Access Authorization Form** - Departments or Agencies are required to file a **System Access Authorization Form (IT-F1001)** when hiring/promoting employees with access to any Information Asset. The form should list which systems and level of access the individual has to each system as well as the technology services that are needed by the employee including, cell phones, tablets, laptops, virtual private network connections, email accounts etc.

2. Network Protection

- 2.1. The Information Technology Department must approve connecting any devices to any Madison County networks owned, leased or operated by Madison County, KY. This includes PCs, network hubs or switches, printers, handhelds, scanners, remote connections, and wireless or wired devices. The use of personal routers and wireless access points on the Madison County, KY network is prohibited.
- 2.2. The installation, removal, or altering of any software on Madison County, KY owned or operated IT Assets is prohibited without authorization from the Information Technology Department or designee.
- 2.3. Smart Phone Devices either owned or operated by Madison County, KY or personally owned Smart phones (Internet and/or e-mail capable cell phones or tablets can be connected to County Email System after Information Technology Department approval). Individuals who connect their personal smart phones to the County email system are granting the right for Madison County, KY to remotely wipe all data from the device if the device is believed to be lost, stolen or has been compromised.
- 2.3.1. Employees with personal Smart Phone Devices connected to the Madison County, KY network must sign the Personal Device Authorization Form (**IT-F1000 – Personal Device Authorization Form**) prior to connecting their device to the Madison County, KY network.
- 2.3.2. All Employees are required to report to the Information Technology Department if their Smart Phone/Tablet or other device (Personal or County Owned) is believed to be lost, stolen or otherwise compromised. Employees should use the Lost or Stolen Device Form (**IT-F1003 – Lost or Stolen Device Form**)
- 2.3.3. All Smart Phone Devices either owned or operated by Madison County, KY or personally owned equipment that connect to the County Email System will be required to have a minimum of a 4 digit password, biometric scan, or security pattern to unlock the device.
- 2.3.4. At no time will the Information Technology Department provide support for personally owned smart phones or wireless devices or will Madison County Fiscal Court be responsible for the information lost on a personally owned device do to a remote wipe by Madison County, KY.

- 2.4. Exploiting or attempting to exploit any vulnerability in any application or network security is prohibited. Sharing of internal information with others that facilitates their exploitation of a vulnerability in any application or network security is also prohibited. It is also prohibited to knowingly propagate any kind of spyware, and/or denial of service attack or virus onto the Madison County, KY owned or operated networks or computers. Individuals who encounter or observe vulnerability in any application or network security must immediately report it to the Information Technology Department.

Disabling, altering, over-riding, or turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden. This includes the installation of any software designed to circumvent security measures.

- 2.5. Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to individuals and Madison County, KY.
- 2.6. Access to any Madison County, KY owned or operated network via VPN requires approval from the Information Technology Department and the Agency or Department Head by granting access by filling out or updating the **Access Authorization Form (IT-F1001)**. VPN accounts will be audited quarterly, accounts not actively being used will be deactivated or removed. Reactivation of intermittently used VPN accounts for vendor support purposes will be accommodated upon request. VPN users must have commercial up-to-date anti-virus software. Vendors accessing any Madison County, KY network via VPN must adhere to any rules or stipulations put forth by the Information Technology Department.
- 2.7. At least annually, departments need to review and approve network accounts for their applications and data. Unless prior arrangements have been made accounts not actively being used, regardless of system, will be deactivated and removed if not accessed at least once every 45 days. All data pertaining to said accounts will be permanently removed 30 days after closure. The Information Technology Department will assist as needed in doing these reviews.

3. Administration, Reporting and Violations

3.1. Administration:

- 3.1.1. The Information Technology Department in conjunction with all Departments and Agencies share the responsibility to enforce the Information Security Policy and report known or suspected violations of this policy.
- 3.1.2. The Information Technology Department holds the responsibility of recommending guidelines that are enforceable, provide monitoring of the technology resources for policy violations and will report policy violations to the Director of Human Resources and the County Judge Executive and the Department or Agency Director.
- 3.1.3. Departments and Agencies have the responsibility to assist in the development and adoption of Policy Initiatives. Department of Agency Directors are responsible for disciplinary actions in response to any violation of the Information Security Policy.

3.1.4. Departments of Agencies may adopt their own Information Security Policy but will be considered in addition to this policy, at no time will it supersede this policy.

3.2. **Violations:** Any Agency or nonaffiliated third party that maintains or possesses personal information regardless of the form must implement, maintain and update information security procedures and practices which includes taking any corrective action to protect and safeguard against security breaches.

3.2.1. Any Agency or nonaffiliated third party must have a reasonable security and breach investigation procedures and practices established and implemented that align with the Department of Local Government as defined in KRS 65.310. They must also follow and comply with any additional requirement under KRS, Federal law, protocols or agreements relating to the protection and privacy of personal information.

3.2.2. If a nonaffiliated third party is required by federal law or regulation to conduct security breach investigations or to make notifications of security breaches, or both, as a result of the nonaffiliated third party's unauthorized disclosure of one or more data elements of personal information that is the same as one (1) or more of the data elements of personal information listed in subsection (6)(a) to (f) of Section 1 of this Act, the nonaffiliated third party shall meet the requirements of Sections 1 to 4 of this Act by providing to the agency a copy of any and all reports and investigations relating to such security breach investigations or notifications that are required to be made by federal law or regulations. This subparagraph of this paragraph shall not apply if the security breach includes the unauthorized disclosure of data elements that are not covered by federal law or regulation but are listed in subsection (6)(a) to (f) of Section 1 of this Act.

3.2.3. **Security Breach** is defined as The unauthorized acquisition, distribution, disclosure, destruction, manipulation or release of unencrypted or unredacted records or data that compromises the agency or nonaffiliated third party and reasonably believes may compromise the security, confidentiality or integrity of personal information and result in the likelihood of harm to one or more individuals OR The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.

1. Security breach does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency if the personal information is used for a purpose related to the agency and is not subject to unauthorized disclosure.

3.2.4. For any agreements executed or amended after January 1, 2015; any agency that contracts with a nonaffiliated third party that discloses personal information to the nonaffiliated third party shall require as part of the agreement that the nonaffiliated third party implement, maintain and updated a security and breach investigation procedures.

3.2.5. The nonaffiliated third party's policy must be appropriate to the nature of the information disclosed and are at least as stringent as the practices referenced in section 1b of House Bill 5.

3.2.6. Nonaffiliated third party's that are provided access to personal information by an agency or collects and maintains personal information on behalf of an agency **shall** notify the agency in the most expedient time possible and without unreasonable delay but within 72 hours of determination of a security breach relating to personal information.

3.3. Reporting: Any agency that has personal information that determines or is notified of a security breach relating to personal information shall as soon as possible but within 72 hours of determination or notification of the security breach do the following:

3.3.1. Required Notifications:

1. Notify the Commission of the Kentucky State Police, the Auditor of Public Accounts and the Attorney General and the Commissioner of the Department for Local Government.
2. Begin conducting a reasonable and prompt investigation in accordance with the security and breach investigation procedures and practices.
3. If the agency determines that a breach has occurred and that misuse of personal information has occurred or is reasonably likely to occur the agency must do the following:

Within 48 hours of completion of the investigation notify in writing all officers listed in 1(a) 1. Of House Bill 5 and the Commissioner of the Department for Libraries and Archives unless provisions of subsection 3 of policy apply. (Law Enforcement has requested not to notify) Complete Form COT-F012.

Within 35 days of providing notifications to the above all individuals impacted by the breach unless bound by subsection 3 of policy apply and if the number of individuals to be notified exceeds one thousand the agency shall notify at least 7 days prior to providing notice to individuals, notify the Department for Local Government.

If the agency determines through the investigation that the misuse of personal information **has not occurred** and is not likely to occur the agency is not required to give notice but shall maintain records that reflect the basis for its decision and retain the record in accordance with the retention period set by KRS 171.420 The Agency must notify the appropriate entities listed in subsection (1) (a) 1. That the misuse of personal information has not occurred.

3.3.2. Notify impacted individuals:

1. Conspicuous posting of the notice on the Agency Website. Notify regional or local media if localized incident Notify major statewide media if widespread incident.
2. Personal Communication to individuals whose data has been breached using one the following methods if the agency has the information available:

In writing, sent to the most recent address reflected in the records of the agency.

By electronic email, sent to the most recent electronic mail address reflected in the records of the agency, unless the individual has communicated to the agency that they do not want email notification.

By telephone, to the most recent telephone number for the individual as reflected in the records of the agency.

3. The notice shall be clear and conspicuous and include the following:

Description of the information that were subject to the breach including the elements of personal information that were believed to be acquired.

Contact information for the notifying agency, including address and telephone number.

A description of the general acts the agency (excluding disclosure of defenses used to protect the information) to protect the personal information from further breach

Phone Numbers, Address and website address along with a statement that the individual can obtain information about steps the individual may take to avoid identify theft , for:

- a. Major consumer credit reporting agencies
- b. Federal Trade Commission
- c. Office of the Kentucky Attorney General

Agency providing the notice shall cooperate with any investigations conducted by any of the agencies notified under this policy along with the office of consumer protection, attorney general, consumer credit reporting agencies and recipient of the notice, to verify the authenticity of the notice.

Notifications can be delayed at the request of a law enforcement agency. Required notices may also be delayed if the agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented with the timeframe established by the policy, this will need written approval from the Attorney General's Office, notifications will be made immediately after these actions have been completed. This does not apply to information that is of the following:

Personal Information that has been redacted, Personal information disclosed to Federal, state or local Governments including Law Enforcement, Court System, or their agents, assigns, employees, or subcontracts to investigate criminal conduct. Personal information that is public and lawfully made available to the general public from federal, state or local government records. Personal information that an individual has consented to have public disseminated or listed or any document recorded in the records of either the County Clerk or Circuit Clerk.

Department of Information Technology
Madison County, Kentucky

Policy Number: IT-02.100

Effective Date: 10/10/2016
Revision Date: 09/08/2016
Next Review Date: 07/01/2018

Subject: User ID and Password Policy

Applicability: This policy is to be adhered to by all departments, agencies and all persons who have, or are responsible for an account on any system owned by Madison County Fiscal Court or managed by the Madison County Department of Information Technology.

Maintenance: The Department of Information has the responsibility for the maintenance of this policy. This policy will be reviewed at least every two years.

Responsibility: Departments, agencies and all staff outlined in the Applicability section are required to understand and follow the guidelines set forth in this document. Each department or agency is responsible for assuring that their staff have been made aware of the provisions and that compliance is expected. Departments, agencies and staff shall also be aware that the intentional, inappropriate use may result in disciplinary action up to and including termination. Agencies that fail to comply may result in service charges to the agency for Madison County Fiscal Courts efforts to remedy the actions resulting from inappropriate User ID and Password usage.

Purpose: The purpose of this policy is to establish a standard for creation of strong passwords, protection of passwords and to describe the responsibilities and procures to follow in relation to all aspects of User Identification (ID) and Passwords.

Policy: Users are responsible for assisting in the protection of the systems they use. The integrity and secrecy of an individual's password is a key element of that responsibility. Each individual has the responsibility for creating and securing an acceptable password per this policy. Failure to conform to these restrictions may lead to the suspension of IT services.

Ownership: User IDs will be unique and assigned to a single employee. Shared user accounts shall only be used in the extraordinary case when it is not operationally feasible to do otherwise, and the risk of using shared accounts is at an acceptable level. The assigned individual for the shared account is still fully responsible for all activity in that account.

Confidential: It is the responsibility of everyone to keep his or her passwords secret. Passwords are considered confidential information and shall not be shared or transferred to others. Passwords must not be written down, or otherwise posted, where they could be seen or interpreted easily by others.

User-level Passwords: are for individuals that fall inside the Applicability of this policy and have access to information stored on systems owned or managed by Madison County, KY. User-level passwords are intended for employees who have access to files and services but have no administrative authority of the management or security of the data, equipment or systems.

User-level Password Creation Guidelines

- Changed at least every 90 days;
- Be eight (8) or more characters;
- Contain both upper and lower case letters;
- Contain at least one number (example 0-9);
- Contain at least one special character (example; !(#&\$(@)~\=);
- Passwords cannot be used more than once in a twelve (12) month period;
- **DO NOT USE** words that can be found in a dictionary, including foreign languages;
- **DO NOT USE** personal information (example: birthdates, addresses, phone numbers, children)

System-level Passwords: are for individuals that fall inside the Applicability of this policy and have access to information stored on systems owned or managed by Madison County, KY. System-level passwords are intended for employees who have access to files and services and also have administrative authority of the management, security of the data, equipment or systems.

Critical/Sensitive Password Creation Guidelines

- Changed at least every 90 days;
- Be twelve (12) or more characters
- Contain both upper and lower case letters;
- Contain at least one number (example 0-9);
- Contain at least one special character (example; !(#&\$(@)~\=);
- Passwords cannot be used more than once in a twelve (12) month period;
- **DO NOT USE** words that can be found in a dictionary, including foreign languages;
- **DO NOT USE** personal information (example: birthdates, addresses, phone numbers, children)

Device-level Passwords: are for administrative logins on devices or services that fall inside the Applicability of this policy and have access to information stored on systems owned or managed by Madison County, KY. Device-level passwords are intended for service accounts, device passwords, domain administrator and enable or sudo passwords. When console passwords can be different than enable passwords, two separate passwords that meet the Device-level password creation guidelines must be used.

Device-level Password Creation Guidelines

- Changed at least every year;
- Be twelve (12) or more characters
- Contain both upper and lower case letters;
- Contain at least one number (example 0-9);
- Contain at least one special character (example; !(#&\$(@)~\=);
- Passwords cannot be used more than once in a twelve (12) month period;
- **DO NOT USE** words that can be found in a dictionary, including foreign languages;
- **DO NOT USE** personal information (example: birthdates, addresses, phone numbers, children)

Administrative-level Passwords: are for administrative accounts that fall inside the Applicability of this policy and have administrative access to information stored on systems owned or managed by Madison County, KY. Administrative-level passwords are intended for employees who are given administrative access to manage the security or authentication to IT Resources. In the case that a service/software where the passwords creation guidelines cannot be meet the maximum level of the service/software account must be used.

Administrative-level Password Creation Guidelines

- Changed at least every year;
- Be sixteen (16) or more characters
- Contain both upper and lower case letters;
- Contain at least one number (example 0-9);
- Contain at least one special character (example; !(#&\$(@)~\=);
- Passwords cannot be used more than once in a twelve (12) month period;
- **DO NOT USE** words that can be found in a dictionary, including foreign languages;
- **DO NOT USE** personal information (example: birthdates, addresses, phone numbers, children)

Password Protection: Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Madison County, KY information. Passwords must not be inserted into email messages or other forms of electronic communication or be revealed over the phone to anyone. Any user suspecting that his/her password may have been compromised must report the incident to the Information Technology and change it immediately.

- **DO NOT** write passwords down and store them anywhere in your office.
- **DO NOT** store passwords in a file on a computer system or mobile device without encryption.
- **DO NOT** use the "Remember Password" feature of applications.

When choosing passwords, all users should avoid using their name, pet's name, relative's name or other common names, user ID, dictionary words (including words from foreign language dictionaries), drowssap (password spelled backwards), not be a set of adjacent keyboard keys (e.g., POIUY), birth date, phone number, address, or any other type of personal information or that which is easily derived from such information.

All User passwords shall be changed at regular intervals as listed in this policy based on level of access. The system will prompt you before the password is set to expire giving all users the opportunity to change their password prior to the expiration date. A password history file shall be implemented to disallow the reuse of recently used passwords. A password history file of the four (4) most recently used passwords shall be kept of all accounts.

After four (4) consecutive unsuccessful logon attempts, user accounts will be locked out for a period of at least 15 minutes. Systems will be monitored for login failures.

All systems that are capable of an inactivity timeout shall lock the device after fifteen (15) minutes of inactivity. Users will have to re-authenticate after the timeout period.

Password Protocol Executive Summary

Passwords are an important aspect of computer security. They are the first line of protection for user accounts, systems and networks. A poorly chosen password may result in the compromise of Madison County, KY Information Assets. As such, all users of a Madison County, KY or a system managed by Madison County, KY are responsible for taking the appropriate steps, as outlined in this policy, to select and secure their passwords.

Department of Information Technology
Madison County, Kentucky

Policy Number: IT-03.100

Effective Date: 10/10/2016
Revision Date: 09/06/2016
Next Review Date: 07/01/2018

Subject: Media Sanitization

Purpose: The purpose of this policy is to protect Madison County, KY Data from unauthorized access or disclosure. This policy will define the requirements for permanently removing data from various media before the disposal or reuse of such media. This process is called Media Sanitization. Failure to properly remove all data may result in unauthorized access to Madison County, KY Data, breach of software license agreement and or the violation of state or federal data security and privacy laws.

Maintenance: The Department of Information has the responsibility for the maintenance of this policy. This policy will be reviewed at least every two years.

Applicability: This policy is to be adhered to by all departments, agencies and all persons who have, or are responsible for an account on any system owned by Madison County Fiscal Court or managed by the Madison County Department of Information Technology.

Responsibility: Departments, agencies and all staff outlined in the Applicability section are required to understand and follow the guidelines set forth in this document. Each department or agency is responsible for assuring that their staff have been made aware of the provisions and that compliance is expected. Departments, agencies and staff shall also be aware that the intentional, inappropriate use may result in disciplinary action up to and including termination. Agencies that fail to comply may result in service charges to the agency for Madison County Fiscal Courts efforts to remedy the actions resulting from inappropriate Media Sanitization.

Roles: The Madison County Department of Information Technology is responsible for ensuring that all Madison County, KY Data is properly removed or destroyed from media before it leaves the control of Madison County Fiscal Court for reuse or disposal.

Definitions:

Degaussing: Demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

Disintegration: A physically destructive method of sanitizing data; the act of separating into component parts.

Incineration: A physically destructive method of sanitizing media; the act of burning completely to ashes.

Media: Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.

Media Sanitization: The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

Purging: A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated software exceeds the value to the attacker. A recommended method of purging data is to overwrite it with random data in three or more passes.

Madison County, KY Data: Any data related to Madison County Fiscal Court functions that are a) stored on Madison County Fiscal Court information technology systems, b) maintained by Madison County Fiscal Court employees or contractors

Policy: To prevent unauthorized disclosure of Madison County, KY Data, all media leaving the control of the Madison County Fiscal Court which is destined for reuse or disposal must have all data purged in a manner that renders the data unrecoverable. All media shall be purged at a minimum per the NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization, Appendix A, Minimum Sanitization Recommendations. When media is transferred between Departments or Agencies the appropriate method will be purging of the media prior to reuse or disposal.

Implementation Procedures: While the primary purpose of this policy is to protect Madison County, KY, it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient and cost effective to purge all Data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside Madison County Fiscal Court, all Data must be purged from the media before giving it to the third party.

Specific instructions for different types of media and regulations follow:

- I. **Electronic Storage Media** (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, etc.)
 - a. If purging is done by overwriting the data, the entire media/device must be overwritten with a minimum of three passes.
 - b. Equipment that can store Madison County, KY Data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the Madison County Fiscal Court should have all data storage devices removed before disposition. If the equipment leaving Madison County Fiscal Court control must retain the data storage devices, all Madison County, KY Data must be properly purged.
 - c. The only acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, or incineration.
 - d. Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.
- II. **Paper-Based Media**
 - a. Any paper-based or other hard copy media containing confidential Madison County, KY Data must be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by the Madison County, KY for Secure Disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (1/32"x1/5"). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the institution, an affiliated organization, or an individual. The maximum particle size for media containing internal data is 2x15 mm (1/16"x3/5").
 - b. Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.
- III. **Optical Media** (e.g., CDs and DVDs)
 - a. Optical media containing Madison County, KY Data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

IV. Smartphones and other handheld devices

- a. Mobile devices like Smartphones (e.g., Blackberry or Treo), MP3 players, and even cell phones, store information and often contain personal or other sensitive information. Any Madison County, KY Data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.

V. Other Media Types

- a. For other media and additional guidelines, refer to NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization, Appendix A, Minimum Sanitization Recommendations.

VI. Electronic Protected Health Information

- a. Madison County Departments or Agencies responsible for electronic protected health information covered by HIPAA must also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, Physical Safeguards, part (d), (1) & (2).

VII. Federal Tax Information

- a. Madison County Departments or Agencies handling Federal Tax Information must also have media sanitization and disposal policies and procedures in accordance with IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies.

Department of Information Technology
Madison County, Kentucky

Policy Number: IT-04.100

Effective Date: 10/10/2016
Revision Date: 09/06/2016
Next Review Date: 07/01/2018

Subject: Clean Desk Policy

Purpose: The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

Maintenance: The Department of Information has the responsibility for the maintenance of this policy. This policy will be reviewed at least every two years.

Applicability: This policy is to be adhered to by all departments, agencies and all persons who have access to sensitive/critical information on any media format.

Responsibility: Departments, agencies and all staff outlined in the Applicability section are required to understand and follow the guidelines set forth in this document. Each department or agency is responsible for assuring that their staff have been made aware of the provisions and that compliance is expected. Departments, agencies and staff shall also be aware that the intentional, inappropriate use may result in disciplinary action up to and including termination. Agencies that fail to comply may result in service charges to the agency for Madison County Fiscal Courts efforts to remedy the actions resulting from inappropriate document storage.

Policy:

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the work day.
4. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
5. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
6. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
7. Laptops must be either locked with a locking cable or locked away in a drawer.
8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
10. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
11. Whiteboards containing Restricted and/or Sensitive information should be erased.
12. Lock away portable computing devices such as laptops and tablets.

13. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
14. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Department of Information Technology
Madison County, Kentucky

Policy Number: IT-06.100

Effective Date: 10/10/2016
Revision Date: 09/06/2016
Next Review Date: 07/01/2018

Subject: Access Channel 46

- I. **Purpose:** The purpose of this policy is to set forth the standards and guidelines for the posting of information, video or media files, scheduling of programming, live airings and information ticker to Madison County Fiscal Court's Access Channel 46.

- II. **Policy:** The programming policy for Access Channel 46 (AC46) shall provide Madison County, Kentucky residents with direct, non-editorial, information concerning services, programs, and activities that are open to the public and residents within our community.

This programming is limited to the following: educational content, documentaries, school activities, functions, sporting events, plays, musicals, interviews and assembled montage of materials and non-profit organization advancement. Information on AC46 cannot be utilized as a means of "free" advertising, personal announcements or religious programming. AC46 is not intended as a political forum nor as a mechanism for support for a particular policy, program, or issue not supported by Madison County Fiscal Court.

All content shall be submitted via email ac46@madisoncountyky.us. Submitted attachments should be in the following formats; jpg, png, psd, pdf, doc, docx, ppt, pptx in landscape orientation. Madison County Fiscal Court has the right to accept, reject, modify and authorize any and all content. Utilization of the AC46 for personal gain will not be permitted.

III. **AC46 Mission:**

- a. To promote Madison County, Kentucky and the Madison County Fiscal Court; showcasing the services provided to the community by Madison County Fiscal Court.
- b. To expand community awareness of activities within Madison County, Kentucky that relate to the citizens of Madison County, Kentucky and provide comprehensive information about programs and services.
- c. To widen the dissemination of information on the activities throughout Madison County, Kentucky.
- d. To improve emergency communications in the event of disaster of widespread service disruption.
- e. Create partnerships with schools, the library, historical museum and other not for profit organizations who assist in mission of bettering the community.
- f. To provide information on public health, safety and welfare issues related to Madison County, Kentucky.
- g. To provide the ability of members of the Community to watch live Fiscal Court Meetings and replays of past meetings to help engage citizens in their government.

- IV. **Types of Programming:** AC46 has the ability to offer many kinds of programming to the community through the use of the latest technology to provide live footage as well as archived footage along with a bulletin board scroll for informational purposes.

- a. **Live Broadcast:** Live broadcast coverage of Madison County Fiscal Court Meetings and selected activities. Madison County Fiscal Court is not responsible or liable for words uttered by the public during live broadcast. Also, Madison County Fiscal Court does not have the capability to suppress vulgar or inappropriate language or activities during a live broadcast.

- b. **Tape-delayed broadcast:** Taped events, locally approved productions/series, clips, meetings, documentaries and other special events may be scheduled between other broadcast on AC46 but may not supersede and Live Broadcast.
- c. **Bulletin Board Information:** Character and graphic generated messages related to County Activities, programs, emergency messaging or events. This service will operate 24 hours a day when other programming is not scheduled. Information shown on these slides shall conform to the policy listed in Section II.
- d. **Emergency:** May consist of live, taped or text and graphics programming, shown at any time, as emergency dictates. The purpose of this programming will be to inform residents of emergency situations, and to instruct viewers in evacuation, detour, notification and escape procedures. In the case of an emergency, regularly scheduled programming may be interrupted or canceled.
- e. **Fiscal Court Replay:** Replays of the most current Fiscal Court Meeting will be re-aired every day at 2:00AM, 7:00AM, 12:00PM, 4:30PM, 7:00PM and 10:00PM. An archive of past Fiscal Court Meetings will also be made available on the Madison County, KY Website for residents who do not have cable service.

V. **Programming Restrictions:** Madison County Fiscal Court will not accept sponsor support from any business, entity or individual and will not broadcast programming containing the following

- a. **Political Broadcast** - AC46 is not intended to be used as a partisan political forum by an individual or group, nor as a mechanism for building exclusive support for a particular person, program or issue. Any programming relating to election for public office or advocacy for a particular cause, viewpoint or policy subject to a pending vote or ballot question will not be allowed. The only political broadcast that is permitted is the airing and re-airing of open political forums conducted to introduce candidates to the community or voting instruction media provided by the Madison County Clerk.
- b. **Commercial programming** - No media including paid advertising material, shall not be considered for broadcast on AC46.
- c. **Copyrighted Materials** - Copyrighted material will not be broadcast unless clearances have been obtained, and written proof of such clearance can be presented or attested to by the entity. Copyright issues shall be resolved at the time of material submission to AC46. It is the implied consent from the submitting entity that all content on the media delivered to AC46 has been approved. All liabilities in regard to Copyrighted material will be placed on the submitting entity.
- d. **Bulletin Board** - Slides on this bulletin board will automatically be removed at the expiration of the dated message. Information will be placed on the rotation two (2) weeks prior to the activity date. Information submitted for recurring events shall be the responsibility of the submitting party to notify the Information Technology Department for the removal or changing of the information, incorrect or outdated information on a recurring event slide is the sole responsibility of the submitting party.
- e. **Retransmission** - Retransmission or any unauthorized use of programming in part of whole is strictly forbidden without the written consent from the owner of the programming. Liability will be placed on the individual submitting the programming.
- f. **FCC** - Programming that violated FCC guidelines for access television including; commercial for-profit making enterprises, trade, business announcements, obscene, indecent, libelous or slanderous speech, lottery information or other illegal content is strictly prohibited.
- g. Any material broadcast on AC46 may be modified or removed at any time when such material is deemed necessary by the Madison County Fiscal Court to be in violation of any of these policies or causes harm or detriment to the Community.

VI. **Programming Disclaimer:** Any videotapes of public meetings, activities or any other events are to be considered unofficial and are not intended to serve as an official record of these events. The views and expressions recorded and/or broadcast during any public event or informational program by speakers and others are not necessarily those of Madison County Fiscal Court its officials, employees and/or agents but are those of the individuals who have made them. Should human error result in the broadcast of incorrect information over AC46, Madison County Fiscal Court its officials, employees and/or agents shall not be liable for the inaccuracy of the information.

VII. **Media Format Specification:** the following formats shall be used to submit media files.

- a. **Bulletin Board-** Power Point, JPEG, PNG, PDF, DOC, DOCX. Other formats maybe accepted. You will be notified if the format is not accepted by AC46.
- b. **Video Format-** All videos should be in standard DVD format. Madison County, KY will not edit or modify any video files submitted. If part of the submitted video is not to be aired the entire submission will be denied.
- c. All media must be clearly labeled with a minimum of program title, individual name and phone number, contact person and requested airing dates.
- d. Madison County, KY highly recommends users make copies any and all materials submitted for broadcast prior to submission. Submitted materials will not be returned.
- e. Airtime is not guaranteed and scheduling is at the discretion of Madison County, KY.