Information Technology Use and Security Procedures

This policy documents the processes and procedures that involve the County's technology assets as managed by the Meade County IT Department. This policy does not purport to address every information technology operating and security issue. Should a user identify an issue or situation that is not addressed in this policy, they should consult their supervisor or contact the County Information Technology Department (IT) for guidance. The Meade County Board of Commissioners may adjust this policy at any time.

1.0 DEFINITION

Information Technology is defined as any equipment, or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Technology Assets are defined as all hardware, software, networks, data, automation services, tools or devices owned by or licensed to Meade County and available for Meade County Government's "official use" in its Information Technology needs. Technology Assets include, but are not limited to, desktop computers, laptop computers, terminals, mobile devices, telecommunications equipment and all related peripheral equipment and software. County technology assets also include voice mail, Internet connectivity, County owned or licensed software applications, email, and all County data and information, regardless of where it is stored:

An **Authorized User** is defined as any individual who has been authorized to use County technology assets. Authorized users have reviewed and signed the Meade County Employee Handbook Acknowledgment form. An authorized user could be either a full-time or part-time County employee, or a non-employee who has been granted authority, to access County technology assets.

The **Cloud** is a network of remote servers hosted on the Internet and used to store, manage, process, and transfer data.

Cloud Services include any application or service provided to a customer that is hosted on a CSP' s infrastructure.

Personally Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information. Each category of information used by the County requires a case-by-case assessment of the specific risk that an individual can be identified. Be aware that non-PH can become PII whenever new information is made available, and can be linked to the preexisting information to identify an individual.

2.0 GENERAL GUIDELINES

a. Unacceptable Use

Under no circumstances is it permitted to utilize computers that are non-county issued/owned/leased, or use any computer that does not have county managed endpoint protection installed and running on them while using secure portions of Meade County's Local Area Network.

- Meade County vendors preforming work on Meade County systems will be allowed access after defining the scope, and duration of their access and determining the fitness of their hardware for connection.

b. Acquisition of Technology Assets

IT is responsible for maintaining the County technology assets, such as networks, desktop, laptop, or tablet computers, servers, printers, peripherals, mobile devices, software, and cloud services, as well as ensuring that these technology assets are acquired and maintained at reasonable costs. All technology assets must be purchased by IT and funded by the receiving departments budget.

This Process is intended to provide:

- a centralized point of information regarding technology assets
- a County wide inventory of hardware and software
- pricing advantages
- software license compliance
- software media storage and management
- hardware and software integration/compatibility assurance

c. Facility Department Work Request System

Authorized users must utilize the Facility Work Request System to request IT services or equipment.

d. Protect Your Computer Equipment

All authorized users share in the responsibility to protect County technology assets from physical and environmental damage, loss and theft. Users are responsible for the correct operation and physical security of the County's technology assets. Destruction, theft, alteration, or any other form of sabotage of County technology assets is prohibited and will be investigated and prosecuted to the fullest extent of the law.

Authorized users must immediately notify IT in writing if any technology asset assigned to them has been damaged, lost or stolen.

e. Use Only Approved Software

Software installed on and/or used by County desktop/laptop computers must be approved and installed by IT. IT will maintain all County approved software media, licenses and documentation. County licensed software may only be reproduced by IT personnel in accordance with the terms of the software licensing agreements.

f. Computer Hardware Configuration Changes

Only IT can authorize configuration changes to any computer hardware. Only IT personnel can install or replace technology related hardware.

g. Guard Against Computer Viruses

All computers shall have IT Department virus scanning software installed and users shall allow scheduled scans on all files on the computer and attached media.

Authorized users who are issued County laptops and tablets are required to connect to the Meade County Government network on a monthly basis. When a laptop is connected to the network, the latest anti-virus and system updates are automatically downloaded.

h. Information Security Awareness Training

Authorized users must complete the County's online Information Security Awareness Training. The purpose of the training is to educate employees about information security awareness and provide best practices to help ensure the protection of County technology assets from unauthorized use. Authorized users will receive automated emails when they are due to take the IT Security Awareness Training. New or updated training modules will be released when deemed necessary.

2.1 County Information and Data

a. Ownership

Meade County Government shall own all rights, title, and interest in its information and data regardless of where it is stored.

b. PII

Authorized users must follow all applicable laws and regulations concerning the use and protection of all PII to which they have access.

c. Storage and Protection

Authorized users are responsible for the protection of essential data files and the security of County information. Storing files and information on the desktop or laptop computer hard drive, a mobile device, or in the cloud, does not ensure protection or security of the information. IT does not backup desktop or laptop computer hard drives, mobile devices or information stored in the cloud.

• All County information must be stored on the Meade County Government network or an authorized infrastructure. Data shall not be uploaded to any other infrastructure, unless approved specifically for storing Meade County data.

2.2 Internet

a. Internet Use/Access

Internet use/access is for official Meade County Government business except as provided for in 2.0(e).

b. List Server/Mailing List Subscriptions

Authorized users will not subscribe to any non-work-related list servers or mailing lists without prior Department Head authorization.

c. Inappropriate Website Access

Authorized users will not access violent, pornographic or other inappropriate websites through the Internet, except for the purpose of investigation. Authorized users will not access any chargeable website without prior Department Head authorization.

2.3 Cloud Services

a. Cloud Services Use/Access

Use only approved and managed Cloud Services.

- Authorized users shall only use Cloud Services that have been approved for County business use by the Meade County Commissioners, and approved as compatible by Information Technology Department.
- Authorized users shall only use County approved user accounts to access a Cloud Services infrastructure for County business use. The use of unapproved user accounts to store County owned information is not permitted.
- Authorized users shall only use County approved methods or tools to access a Cloud Services infrastructure for County business use.

2.4 Violations

Misuse of Meade County's technology assets or breaches of IT security is a violation of this policy and may result in disciplinary action, up to and including termination of employment.

2.5 Separation of Employment

Upon separation of employment from Meade County, all County-owned IT equipment provided to an authorized user must be returned in good and usable condition no later than the last day of employment. If the equipment is not returned or is returned damaged and unusable, the cost of replacing the equipment may be withheld from the employee's final paycheck under the terms of the Federal Fair Labor Standards Act (FLSA).

Prior to separation of employment with Meade County, authorized users must remove passwords from any County files and decrypt any files which they have encrypted.

3.0 POLICY ADMINISTRATION AND REVIEW

3.1 Administrator Access and Monitoring

All files on County devices or networks (including email) and all phone records of County owned telephones are the property of Meade County Government. Authorized users understand that they do not possess a "right to privacy" in County email or phone communications.

An IT Administrator may only access authorized users mailboxes, telephone records or network activity for any maintence or troubleshooting purpose, including, but not limited to, the following:

1. To retrieve lost messages,
2. To recover from system failures, or
3. To monitor system performance.

At the written direction of the legally authorized entity, an authorized user's email, Internet usage, network activity or telephone records may be monitored for any valid business-related purpose, including, but not limited to, investigation of the following:

1. Excessive personal use,
2. Violation of federal, state or local law, or
3. Personnel issues or violation of County policy.

3.2 Supervisor and Department Responsibilities

a. Monitoring Usage

All supervisors within the County departments are responsible for ensuring that their authorized users are aware of, and adhere to, these policies and procedures.

b. Notifying IT

Departments are responsible for providing notification to IT via the IT Work Request System when an authorized user begins, changes or ends employment with Meade County. If a department requires the immediate termination of an authorized user's access to County technology assets, the appropriate departmental representative should notify IT by phone and then document the request via the IT Work Request System.

4.0 EXCEPTIONS

Provisions of this policy may be waived at the discretion of the Meade County Commissioners. Any and all exceptions to this policy must be approved in advance.