ARTICLE I – INTRODUCTION

Jo Daviess County provides a variety of information technology (IT) resources to its employees and officials to improve public services and maximize efficiency. In order to make best use of these IT resources, Jo Daviess County has developed this policy to serve as a guide for Jo Daviess County employees and officials who utilize the County’s IT resources.

All employees and officials who have access to County IT resources are required to read and comply with this County policy. Failure to do so may result in revocation of access to information technology resources and/or disciplinary action ranging from a reprimand to immediate termination.

1.01 Policy Goals

It is the goal of this policy to:

- Support the overall duties and responsibilities of Jo Daviess County Government
- Protect confidential information of the County, exempt from FOIA, from theft or unauthorized disclosure to third parties
- Prevent the waste of IT resources
- Reduce, and if possible, eliminate potential legal liability to employees, the County, and third parties
- Ensure the availability of IT resources to all County employees and officials
- Serve as a guide to all County employees and officials as to proper use of IT resources

1.02 Jo Daviess County IT Staff Guiding Principles

Jo Daviess County IT staff will strive to:

- Ensure the availability and security of the County’s networks and information
- Provide quality, professional, and customer focused services and solutions to County employees, officials, vendors and the public
- Achieve the standardization of technology solutions, whenever feasible
- Maximize the County’s information technology investments by leveraging solutions and services to the fullest extent possible

ARTICLE II – DEFINITIONS

The following definitions apply to the context of this policy:

2.01 Attachments - files created in other applications (such as a word processor or spreadsheet) that are incorporated into an e-mail message.

2.02 Blog - publicly accessible web forum that contains an online personal journal with reflections, comments, and opinions; which often solicits commentary from readers or provides hyperlinks to other online resources.

2.03. Blogging - the act of updating or contributing to a blog.
2.04. Criminal Justice Information System (CJIS) – a federal program operated by the Federal Bureau of Investigation (FBI) which collects and distributes criminal justice information to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment and licensing agencies concerning individuals, stolen property, criminal organizations and activities, and other law enforcement-related data.

2.05. E-mail - an electronically transmitted message, along with any attachments and any information appended by the e-mail system.

2.06. E-mail System – a system that allows users to send, receive and store messages and files with other individuals or groups of people over an internal computer network (Intranet) or the Internet.

2.07. Encryption - a means of coding messages so they appear to be random characters. Encryption prevents disclosure of sensitive information to unauthorized third parties and allows for authentication of the information sent.

2.08. Firewall – a firewall is used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet. A firewall may be implemented using hardware, software, or a combination of both.

2.09. File Transfer Protocol (FTP) – a standard network protocol used for the transfer of computer files between a server and client computer. FTP is commonly used when a file it too large in size to transfer as an email attachment.

2.09. Flash Drive – also known as a thumb drive or USB drive is a small removable electronic device containing flash memory that is used for storing data or transferring it to or from computers and other devices.

2.10. Freedom of Information Act (FOIA) – Under the Illinois Freedom of Information Act (5 ILCS 140), records in the possession of public agencies may be accessed by the public upon written request. Pursuant to Section 2 (c), “public records” are all records, reports, forms, writings, letters, memoranda, books, papers, maps, photographs, cards, tapes, recordings, electronic data processing records, recorded information, and all other documentary materials, regardless of physical form or characteristics, having been prepared or having been or being used, received, in the possession of or under the control of any public body.

2.10. Freeware – software that is free to use but is still copyrighted and may include a license agreement that restricts usage or distribution.

2.12. Health Insurance Portability and Accountability Act (HIPPA) – a US law designed to provide privacy standards to protect patients’ medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

2.13 Home Network Folder – a network storage location assigned to a specific user and not shared with other users on the network. Typically designated by the drive letter H:


2.15. Information Technology (IT) System – an organized system of computer hardware, software, and connecting devices used for the collection, storage and communication of electronic information.

Approved 11.13.18/Replaces Information Resources Acceptable Use 05.05.08, Computer Network 05.13.08, Government Website 11.11.04, & Remote Access 04.13.09
2.16. **Intranet** – a private, internal network accessible only to an organization’s staff that provides a wide range of information and services.

2.17. **Internet** – a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols; also called the World Wide Web.

2.18. **Internet Browser** - an application which displays Web Pages and other information found on the Internet. Commonly used browsers include Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera, and Safari.

2.19. **Information Technology (IT)** – the technology involving the development, maintenance, and use of computer systems, software and networks for processing, storing, retrieving and sending data.

2.21. **Malware** – malicious program or code intended to do damage to any part of an Information System

2.22. **Mobile Device Management (MDM)** – software systems used to secure mobile devices and enforce policy through remotely managed device control.

2.23. **Mobile Device** – any device used to access Jo Daviess County’s information resources from outside of the County’s secure facilities or via any network connection other than Jo Daviess County’s private, secure network facilities.

2.24. **Network Storage Location** – a network folder, database, file share, inbox, mapped drive, cloud storage or other network storage provided for the purpose of storing electronic information on a secure computer network. Such locations are secured and regularly backed up to protect against data loss. Local device storage is not a Network Storage Location.

2.25. **Outlook Web Access (OWA)** – a web-based e-mail client that County employees and officials may use to access their e-mail through a web browser from any Internet connection. OWA provides most of the same functionality found in Outlook.

2.26. **Personal Mobile Device** – any device not owned or provided to the employee or elected official by Jo Daviess County

2.27. **Protected Information** - Any information that is considered private, confidential, proprietary or sensitive for which access or release is restricted by policy, rule, regulation or law.

2.28. **Public Resource** - Includes not only County equipment, hardware, software or tangible articles, but also the employee’s time expended while on duty with the County.

2.29. **Removable Storage Media** – Any storage device that is portable and can be used to transfer information from one computer to another. (Flash Drives, SD Cards, CDs, DVDs, etc.)

2.30. **Risk** - Those factors that could affect confidentiality, availability, and integrity of Jo Daviess County’s information assets and systems

2.31. **Shared Network Folder** – a network storage location shared by a group of users on the network, particularly a department or office. Typically designated by the drive letter I:

2.32. **Shareware** - Software that is distributed free on a "trial basis" with the understanding that the user may need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date

Approved 11.13.18/Replaces Information Resources Acceptable Use 05.05.08, Computer Network 05.13.08, Government Website 11.11.04, & Remote Access 04.13.09
(after 30 days, the user can no longer get access to the program). Other shareware (sometimes called liteware) is offered with certain capabilities disabled as an enticement to buy the complete version of the program.

2.33. **Spyware** – rogue software used by advertisers and others to collect information or interface to other applications without the end user’s knowledge.

2.34. **Social Network** – publically accessible website or application which allows individual to create profiles for the purpose of meeting and interacting with each other. Facebook, Snapchat, Twitter, and Instagram are commonly used social networking applications.

2.35. **Social Networking** – the practice of using social network applications

2.36. **Social Media** – an application designed to facilitate social networking (Synonymous with Social Network)

2.37. **Streaming Technology** - a technology that distributes audio or video information from a source over a network to be received to a PC and played back or copied to a file. Pandora and iHeartRadio are examples of streaming audio websites. YouTube is a commonly used video-sharing website.

2.38. **Third Party** – Any individual from an outside source (contracted or otherwise) who requires access to Jo Daviess County IT systems for the purpose of performing work. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

2.39. **Uniform Resource Locator (URL)** – indicates the location of a website or resource on the Internet as well as the protocol used to access it; commonly called an "internet address" or “web address.”

2.40. **Users** - Information system end users including: employees, elected officials, vendors, consultants, a third party, and public users.

2.41. **Virus** - A malicious software program or piece of code designed to execute and replicate itself from host to host with typically a harmful effect, such as corrupting a system or destroying data.

**ARTICLE III – SYSTEM ACCESS, SECURITY & USE**

Information technology resources are the property of Jo Daviess County. Access to these IT resources is provided to employees and officials primarily for the purpose of advancing the governmental functions of the County. This includes, but is not limited to:

- Communication with and providing services to members of the public
- Conducting the business of the County department or office
- Communicating with other employees for work-related purposes
- Gathering information relevant to job duties or to expand knowledge and skills

Access to these information technology resources impose certain responsibilities and obligations on all County employees (full-time, part-time, contract and temporary), officials, other government entities, a third party, and companies or individuals, contracted to do work for the County or use County IT resources, referred to herein after as “users.” All users are subject to the policies of the County as well as local, state and federal laws. All data, e-mail, e-mail attachments, documents and other electronic information within the County’s information system are the property of Jo Daviess County. THERE SHOULD BE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY WHEN USING THE COUNTY’S
P2018-10

INFORMATION TECHNOLOGY RESOURCES. The County has the capability and the right to view data and e-mail at any time. This policy does not supersede any state or federal laws regarding privacy, confidentiality and appropriate use.

3.01. System Access and Permissions

Access to County IT systems is granted to users at the request of a department head. Department heads wishing to obtain access or update system access permissions for an employee, must submit an e-mail to County IT staff for the request in advance of the date and time at which the access will be required.

3.02. Systems User Accounts

Users are granted access to the County’s network resources through password protected individual user domain accounts. The following responsibilities apply to all user accounts on any County IT systems:

- A user is prohibited from using any account name other than those he/she is assigned or given authorization to use by the department head
- A user is responsible for all inquiries, entries and changes made to any of the organization’s IT systems using his/her username and password
- A user shall not leave his/her username and/or password where someone else may see or find these credentials; keeping written passwords is discouraged
- A user shall not use his/her username and/or password to log another individual into any County IT systems
- A user shall not store passwords electronically unless they are encrypted and password protected
- Users with access to CJIS data must follow CJIS requirements to be compliant:
  1. Be a minimum length of eight (8) characters on all systems.
  2. Not be a dictionary word or proper name.
  3. Not be the same as the User ID.
  4. Expire within a maximum of 90 calendar days.
  5. Not be identical to the previous ten (10) passwords.
  6. Not be transmitted in the clear outside the secure location.
  7. Not be displayed when entered.

- Users not accessing CJIS data are required to change domain user account passwords at a minimum of once every 120 days. All passwords should be a minimum of six alpha-numeric characters and consist of upper case letters, lower case letters, numbers and symbols; other applications and systems may require password changes at different intervals
- User passwords are not to be shared except for problem resolution or troubleshooting with authorized County IT staff
- County IT staff will periodically review user permissions and remove permissions no longer in use or required by an individual user
- Department heads are responsible to advise County IT staff of changes to an employee’s job responsibilities which impact the individual’s need for system privileges

3.03. Systems Security

It is the responsibility of every user of Jo Daviess County’s IT systems to ensure the confidentiality and integrity of the information owned or managed by Jo Daviess County. Users should adhere to the following:

Approved 11.13.18/Replaces Information Resources Acceptable Use 05.05.08, Computer Network 05.13.08, Government Website 11.11.04, & Remote Access 04.13.09
All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of data and information at all times

Users are required to monitor workstations or laptops and take measures to prevent unauthorized access and theft

When approached by an individual that may be able to view data or information to which he/she is not authorized, such as CJIS or HiPPA information, users are to minimize the system display or otherwise secure it so that the individual is not able to view the data or information

The County uses a network firewall device that maintains a list of URLs or websites that are considered malicious and actively blocks such sites. In addition, users must avoid using sites that are not known to be safe and substantially related to their job responsibilities

Software programs and applications installed on County equipment must be licensed

Users shall not remove County-owned computer equipment and peripherals from the premises unless authorized to do so

Users shall not download any software without prior approval from County IT staff; unapproved software shall be removed without advance notice to the user

Users with access to download data are responsible for managing and protecting it from unauthorized access, disclosure, and theft

Users shall not download any data or information from the County’s IT systems to store or use it on any other system or device, other than the device authorized for use

Users shall not open any suspicious e-mails or suspicious website links in e-mails

If uncertain an e-mail is suspicious, contact County IT staff immediately and wait for assistance

If uncertain a website link is suspicious, do not click on it. Contact County IT staff immediately and wait for assistance

Users shall not connect non-County-owned computer equipment or peripherals to the Jo Daviess County network or utilize IT systems or computer equipment not owned by the County, unless County IT staff grants approval for such use

Users shall not make use of tools or techniques to break/exploit or disable security measures on the County’s network

Users shall not change operating system configurations, upgrade existing operating systems, or install new operating systems on County equipment

Users shall not connect to unauthorized networks through the County’s systems or devices

### 3.04. Acceptable Use

Acceptable use is defined as that which is lawful, ethical, reflects honesty, and shows restraint in the consumption of shared resources. The primary purpose for using the County’s information technology resources is to perform the governmental functions of the County.

### 3.05. Inappropriate Use

Users are prohibited from engaging in the following activities, with the exception of those activities required in the fulfillment of a user’s job responsibilities, for which he/she has received prior approval by the appropriate department head and notified County IT staff:

- Use technology resources for personal gain, political purposes, or to support or advocate for non-County related business
P2018-10

- Create, distribute, upload or download any disruptive, abusive, harassing, threatening, or offensive messages; including offensive comments or graphics about sex, race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs, political beliefs, or national origin
- Use technology resources for illegal or unlawful purposes or to support or assist such purposes
- Use technology resources for wagering, betting or selling chances or to support or assist such purposes
- Use technology resources for personal long distance telephone calls
- Attempt to circumvent or subvert system or network security measures, provide internal network access to any unauthorized users or use an account to gain unauthorized access to other networks and systems
- Mount an attack on the security of any system or attempt to hack or introduce viruses into any system
- Use the network in a manner that may disrupt network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses or malware, and sustained high volume network traffic
- Intercept network traffic for any purpose
- Install encryption software on any County-owned computer equipment; a user may not use encryption keys or encryption technology that is unknown to his/her department head and IT staff
- Engage in online fundraising
- Engage in mass-mailing, “everyone e-mails”, or send county-wide messages without department head approval
- Send or forward mailings about viruses or other warnings about outside computer attacks to anyone (these are almost always a hoax and should not be propagated); users should contact County IT staff immediately
- Initiate or forward chain letters by e-mail
- Spoof (disguise) your identity or send anonymous e-mail or send e-mail under another employee’s name
- Forge e-mail header information for any use that does not appropriately and accurately identify the sender
- Download any non-standard or non-business related files or software, including "freeware" and/or "shareware" programs unless previously approved by County IT staff
- Load personal online accounts on County owned equipment
- Disburse or share any County data not authorized by the department head and relevant to the job being performed, or any data considered protected, unless expressly authorized to do so in the performance of one’s job responsibilities
- Make or use illegal copies of copyrighted software or other mediums, store such copies on County systems, or transmit them over the County network
- Any activity not deemed to be in the best interest of Jo Daviess County Government
- Any activity that compromises the security or integrity of Jo Daviess County IT systems
- Any activity that violates any Jo Daviess County ordinance, including the Jo Daviess County Code of Ethics, Federal, State or local laws

It is the responsibility of the department head to be aware of how the County’s information system is being utilized by his/her employees and ensure that employees are periodically informed and aware of this policy. If the department head suspects any employee is violating this policy, they should contact the County Administrator and IT/GIS Director.

3.06. Personal Use

Users shall not use IT resources for personal use. This is defined as any personally initiated computer-based activity (e-mail, internet browsing, storing personal files on County equipment, etc.) that is conducted for purposes other than for County business.
3.07. System Monitoring

All computer applications, programs, data and information, created or stored on county IT systems is the property of Jo Daviess County and may be monitored without prior notice. The County reserves the right to access any information stored, created or received on the County’s IT systems. The reservation of this right is to make certain that public resources are not being wasted, the County’s business is carried out, and to ensure the County’s IT systems are operating as efficiently as possible. Monitoring or access may be exercised under any of the following circumstances:

- Performance testing or problem solving purposes
- As necessary in the course of an investigation for possible violation of County policies
- If there is reasonable suspicion that a user has committed, or is committing a crime against the County or for which the County could be liable
- Random or automated monitoring to ensure that content is in compliance with the County’s established policies
- A request for monitoring made by appropriate authority
- When required to do so by law

ARTICLE IV – E-MAIL & INTERNET USE

4.01. E-mail Use

E-mail allows County employees and officials to send, receive and store electronic messages and files with other individuals or groups of people over the internal County network (Intranet) or the Internet for the sole purpose of conducting County business. Personal use on the County’s e-mail system is prohibited.

Users should employ the same care in drafting e-mail and other electronic documents as they would for any other written communication. Content created should be accurate. Anything created on a County-owned device or personal smartphone with work e-mail account access has the potential to be reviewed by others subject to FOIA.

4.02. E-mail Account Creation and Administration

E-mail account creation, changes or removal must be requested by the department head in advance of the requested action date. User accounts will be archived and deleted after the termination of employment. However, a department head may request a user account be maintained and e-mail forwarded for a period of time, after which the user’s account will be archived and deleted.

4.03. E-mail Account Use and Security

E-mail accounts may be used only by the intended user. Use by anyone other than the named account’s owner is not permitted. It is the account owner’s responsibility to maintain proper password protection and take reasonable precautions to prevent unauthorized use. When an employee is absent for an unanticipated or extended period of time, the department head may request of the IT staff to provide access to the employee’s e-mail account for the purpose of ensuring timely responses to e-mail correspondence.

Jo Daviess County e-mail addresses are not to be used as contact addresses for solicitations, account IDs, chat rooms, social networking, blogs or subscriptions not related to County business.
4.04. E-Mail Encryption for Criminal Justice Information System (CJIS) Requirements

To facilitate the communication of protected CJIS information, users must use encryption for transmission. Encryption is designed to prevent access to confidential or private information by anyone other than the intended recipient.

Unencrypted, unsecured e-mail may be intercepted, forwarded and altered. CJIS information should be sent only by means of the County’s secure, encrypted e-mail system.

4.05. E-mail Records Retention

E-mail and attached documents are the property of Jo Daviess County. Many e-mail messages represent temporary communications that are non-vital and may be discarded routinely. However, depending on the content of the e-mail message, it may be subject to the Freedom of Information Act (FOIA) and Criminal Justice Information System (CJIS). E-mail falling under this category is to be retained indefinitely.

Users are cautioned to be aware that deleting an e-mail message from a mailbox does not delete all copies of the message. The County reserves the right to establish policy that e-mail messages will be retained on the County’s e-mail server for finite period of time, and then deleted.

4.06. E-mail Monitoring & Access

It is not the practice of Jo Daviess County to routinely monitor e-mail activity or content. As necessary, County IT staff may access e-mail accounts for business purposes or at the request of a department head, such as but not limited to:

- System maintenance
- Troubleshooting
- Performance monitoring
- To fulfill FOIA requests
- In the course of a legal investigation

4.07. Outlook Web Access (OWA)

Outlook Web Access (OWA) is a web-based e-mail client that County employees and officials may use to access their e-mail through a web browser from any Internet connection. OWA provides most of the same functionality found in Outlook. CJIS information should not be accessed or transmitted using OWA.

4.08. Internet Use

The Internet is a powerful tool for research, procurement, and communication. Jo Daviess County provides Internet connectivity to users who require it to effectively perform County business.

Only the user(s) assigned to a computer workstation may access the Internet from that workstation using an internet browser. Use by other user(s) to access the Internet constitutes a violation of this policy, unless approved by the user’s department head.

All Internet activity on the County’s network is logged. Jo Daviess County may use this information in the assessment of system performance, troubleshooting and monitoring of appropriate use. The County reserves the right to block access to any Internet site deemed to be malicious or in conflict with any County policy. Inappropriate use of the Internet, as defined in section 3.05, may result in loss of internet access and disciplinary action up to and including termination.

Approved 11.13.18/Replaces Information Resources Acceptable Use 05.05.08, Computer Network 05.13.08, Government Website 11.11.04, & Remote Access 04.13.09
4.09. Internet Safety and Security

Use of the internet incurs certain risks and it is the responsibility of the user to exhibit caution and good judgment when accessing internet content. Some internet websites are infected with viruses, spyware or other types of malware, which may be downloaded to the user’s workstation or laptop without any interaction from the user. The following guidelines should be adhered to when browsing the Internet from County computers:

- Avoid unknown URLs or websites
- Do not install or activate any unexpected installations or downloads
- Do not respond to messages or click on links from unknown sources
- Contact County IT staff immediately if you encounter an unexpected or suspicious download or virus warning

4.10. Objectionable Internet Content

A wide variety of information is available on the Internet. Some users may find this information offensive or otherwise objectionable. Users should be aware that although the County may utilize website filtering to avoid objectionable material, it does not have complete control over the Internet and can therefore not be responsible for the content of information available.

4.11. Blogging

The use of internet blogs on County computers is discouraged unless such use is necessary in the performance of a user’s job responsibilities. Blogging activities on County computers are subject to all provisions of this policy and all other policies of the County.

4.12. Instant Messaging and Chat Rooms

A user may only engage in chat rooms, instant messenger communications or newsgroups if it is required as a part of their job requirements and has been approved by his/her department head and County IT staff.

4.13. Social Networking and Social Media

Unless specifically required in the performance of a user’s work activities, social networking and the use of social network sites, including personal use, is prohibited on County systems. These sites often present security risks due to malware and computer viruses.

4.14. Use of Fee Websites

A user who accesses any Internet sites for which a charge or a fee is involved, without the written consent of that user’s department head, may be held responsible for any and all payments associated with visiting that website.

4.15 Internet Use during Non-Work Hours

Access to the Internet during a user’s non-work hours via County equipment shall adhere to all provisions of this policy and cannot conflict with the best interests of the County.
4.16. High Bandwidth Applications

Accessing entertainment, games and other websites that use significant bandwidth could jeopardize network speed for other business uses, and should be avoided. This includes websites that broadcast radio, TV, video, or any streaming technology, and other similar high-bandwidth sites that are not related to County business.

4.17. Suspension of Internet Access Privileges

User Internet access is at the discretion of a department head and may be suspended at any time. Use may also be suspended in the event of a continued breach of this or any other policies through the internet usage of a specific user. In addition to the suspension of internet access, misuse may result in disciplinary action up to and including termination.

ARTICLE V – NETWORK COMPUTER USE

5.01. Network Computer Use

The Jo Daviess County computer network provides connectivity for all County departments and other government agencies to centrally managed systems. These systems provide: communications, data security, storage and external connectivity via the Internet.

User data and other documents are considered County assets and should be treated as such. For the purpose of protecting these assets, users should store all data files on the network directories provided, as these locations are backed up daily.

5.02. Network Storage

Network user accounts provide access to designated network storage locations. Each individual account is assigned a “Home” network folder, often designated by the drive letter “H:” which is not accessible by other users; and a “Shared” network folder which is shared with other users within the department or business unit. In addition, other storage locations (drives) may be designated for application specific storage.

5.03. Data Backup

Jo Daviess County will provide regular backups of all data stored to designated network storage locations. These backups provide the capability to restore a system or file share in the event of loss due to device malfunction, file corruption or catastrophic system failure. To ensure the successful backup of all critical data, files should only be stored to designated network storage locations and not be stored on user workstations’ or laptops’ local storage locations. Requests for the restoration of accidentally deleted or corrupted files from backup should be made to the County IT staff.

5.04. Attachment of Equipment or Other Devices

Prior approval from the department head and County IT staff must be obtained before any equipment is attached to the County network or to a County computer. Users shall not:

- Connect any devices to the County network without approval from the department head and County IT staff
- Make connection to individual servers /workstations/laptops/peripherals for vendor remote access purposes, without prior approval from the user’s department head and County IT staff

Approved 11.13.18/Replaces Information Resources Acceptable Use 05.05.08, Computer Network 05.13.08, Government Website 11.11.04, & Remote Access 04.13.09
5.05. Removable Storage Media

The use of removable storage media, such as a USB flash drive, presents a risk for the accidental release of confidential or private information and provides a vehicle through which computer malware such as viruses may be spread. Users who have a need to use these devices are cautioned to do so in a manner that reduces these risks and adheres to the following guidelines:

- Use must be approved by the user’s department head and County IT staff
- It is recommended that the device be obtained by County IT staff for the user
- Only non-confidential or public information may be stored on such devices, unless the device is encrypted, password protected and the user has obtained authorization from his/her department head and County IT staff
- The user accepts the responsibility of protecting any information stored on the device
- Devices used to store County information shall not be used for any other purpose
- Lost devices should be immediately reported to the user’s department head and County IT staff

5.06. Unauthorized Software

Use of unauthorized software may degrade the performance of the County’s systems, create security risks, reduce employee productivity and expose the County to liability. Users are prohibited from installing any applications, plugins, or other software on County computer equipment without department head and County IT staff approval prior to installation. Software installations not approved prior by County IT staff may be considered unauthorized and will be subject to removal and disciplinary action to the user. It is the responsibility of all users to comply with maintaining County standards and protecting computing resources by not downloading or installing unauthorized software.

County IT staff will immediately remove any unauthorized software in use, when encountered, unless the software has a legitimate business purpose for the user, is appropriately licensed and approved by the user’s department head.

Violation of Copyright Laws and Policies: According to the US Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $150,000 per work copied, and criminal penalties, including fines and imprisonment. County employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination.

5.07. Mobile Devices

Department heads have the discretion to allow non-work related use of personal mobile devices, such as smartphones, during working hours. Employees should keep personal mobile devices off or silenced and limit their use to breaks and outside of common work areas to avoid disruption.

With department head approval, a user can request County IT staff to configure a personal smartphone to connect to the County's e-mail system for the specific user. Security requirements of a lock screen and PIN or password will apply to personal smartphones connecting to the County’s e-mail system. Users should remember that personal smartphones used for conducting County business are subject to FOIA.

Any device used to remotely access the County’s information resources is considered to be a mobile device under this policy.

Approved 11.13.18/Replaces Information Resources Acceptable Use 05.05.08, Computer Network 05.13.08, Government Website 11.11.04, & Remote Access 04.13.09
5.08. Remote Access

Remote access allows certain users to securely connect to the County’s network from a remote location to conduct County business. Any remote access using VPN (virtual private network), RDP (Remote Desktop Protocol) or any other remote access software to the County network must be approved by the department head and County IT staff. All users by default will have account settings set to deny remote access.

5.09. FTP Access

FTP is an acronym for File Transfer Protocol. As the name suggests, FTP is used to transfer files between computers, typically from an FTP server to a client computer. FTP is commonly used when a file is too large in size to transfer as an e-mail attachment. County meeting packets, budget information, and GIS data are commonly transferred using the County’s FTP site. With department head approval, users may contact County IT staff to setup temporary FTP access to transfer files too large in size to be an e-mail attachment.

ARTICLE VI – RECORDS RETENTION

Jo Daviess County complies with the Illinois Local Records Act (50 ILCS 205/). Department heads are responsible to ensure that records subject to this Act are appropriately retained. Records may be retained in hardcopy or electronic format. For the purpose of this policy, records are presumed to be in electronic format.

The following guidelines relate to the retention of electronic records created on Jo Daviess County IT systems.

6.01. Records Custodian

Each department is responsible for the records created during its regular course of business. Unless otherwise prescribed by policy, ordinance or law, the department head is presumed to be the records custodian for a given department.

6.02. Retention

Retention is the responsibility of the custodian of the record. To retain a record in an electronic format means to store such record to a designated network storage location. Do not store electronic records to a local workstation or laptop hard drive or removable storage location as such storage is subject to loss due to device failure, malfunction or theft.

6.03. System Backups and Archives

System backups and archives are utilized to protect information from accidental loss due to system failure, disaster or accidental deletion. Backups and archives are not intended to be used as the primary repository for records retention. Files deleted from a designated network storage location will also be deleted from backups within a number of days. Likewise, information archives are periodically purged. To ensure the retention of the record in accordance with the designated Act, a records custodian must save a copy in a designated network storage location.

6.04. E-mail Archive

Jo Daviess County provides dedicated e-mail storage archives to better facilitate records discovery for e-mail record requests. As previously stated, archives are not configured to fulfill specific records retention requirements and
custodians are advised to retain copies of any and all records subject to retention in a designated network storage location.

6.05. Records Requests

Records requests, such as FOIA requests, are to be directed to the custodian of the records requested. County IT staff will assist custodians in locating records by utilizing available tools to search for records using dates, keywords and metadata; however, it is the custodian’s duty to fulfill the request. Record requests may also be reviewed by the State’s Attorney Office before any records are released.

ARTICLE VI – IT SUPPORT AND AFTER HOURS SUPPORT PROCEDURES

Most County departments have standard business hours falling between 7:00 am – 4:30 pm, Monday – Friday. County IT staff working hours are typically 6:00 am – 4:30 pm, Monday – Friday. However, specific departments, such as the Sheriff’s Office are 24/7 operations. IT-related issues can occur during non-standard County business hours, weekends, or holidays. The County also recognizes the importance that County IT staff needs time away from work. Therefore, after-hours IT support should be limited to mission critical issues only.

Mission Critical Issues Include:

- Dispatch/Jail unable to function
- E-mail Exchange server not working
- iFiber connectivity is down
- Power outage impacting the network
- Weather-related (i.e. server room flooding of 2011)

County employees and officials should follow these procedures in the event of computer-related problems that occur during non-standard County business hours (8 am - 4 pm, Monday - Friday), weekends or holidays.

Step #1
Determine if the computer-related problem is mission critical. If the issue is NOT mission critical, please send an e-mail to itsupport@jodaviess.org with all pertinent information about the problem. IT staff will work on the problem during standard County business hours.

Step #2
After determining that the problem is mission critical, if the computer-related problem appears to be a software/hardware issue covered by a vendor’s support contract, please first contact that specific vendor’s support team to troubleshoot the issue. If the issue cannot be resolved by the vendor’s support team, proceed to Step #3.

Step #3
After determining that the problem is mission critical and that it appears to be an issue not directly related to a specific software program/hardware covered by vendor support, please contact Jo Daviess County IT staff for support.
ARTICLE VII – COMPUTER TRAINING

7.01. Software Applications Training

Due to the diversity of software applications used throughout the County, it is difficult to have a single training solution to meet the needs of all County employees. For this reason, it is left up to the individual departments to determine the training needs of their employees.

7.02. Security Training

The IT/GIS Director provides periodic system security training to all employees as part of the County’s Quarterly Safety Training.

ARTICLE VIII – DEPARTMENTAL WEB PAGES AND SOCIAL MEDIA SITES

Department specific web pages and social media sites are important tools for the provision of information to the public in a timely and easily accessible manner. Jo Daviess County encourages the responsible use of these tools. The official County website is https://www.jodaviess.org. This website provides a home page for each department. This is to be every County department’s primary web presence and home page. Additional websites and authorized social media portals must link from this official County website.

8.01. Use of Department’s Web Page

All internet content related to a department’s mission is to be included on the departmental web page. The accuracy, quality and timeliness of internet content is the responsibility of the department head. Content changes to a departmental web page should be submitted to webadmin@jodaviess.org so that GIS/IT staff can make the changes.

8.02. Creation of Social Media Sites and Content

A department may elect to create an official department social media site. When doing this, the department must notify GIS/IT staff at webadmin@jodaviess.org and request a link to the social media site be created from the County’s official website. The accuracy, quality, and timeliness of all content on an official department social media site is the responsibility of the sponsoring department. All communications carried out on County equipment or County sponsored electronic media must adhere to the appropriate use guidelines set forth in this policy.

ARTICLE IX – MISUSE REPORTING AND VIOLATIONS OF POLICY

Misuse of the County’s IT resources may occur in many forms. Users must report any misuse of the County’s IT resources to the appropriate department head.

County employees and officials who violate this policy may have their access removed and may be subject to disciplinary action up to and including termination. In addition, contractors or other third party(s) who violate this policy may have their contract revoked. Other legal remedies, including criminal prosecution, may also be pursued if warranted.

It is the policy of Jo Daviess County to handle violations as follows:

1. The violation should be reported to the user’s department head.
2. The department head should inform the County Administrator and IT/GIS Director and of the violation.

Approved 11.13.18/Replaces Information Resources Acceptable Use 05.05.08, Computer Network 05.13.08, Government Website 11.11.04, & Remote Access 04.13.09
3. The department head should approach the violator(s) directly with the findings, ensure the user is aware of this policy, and give the opportunity to cease and desist; or, depending on the severity, follow disciplinary procedures consistent with the guidelines and policies of the “Jo Daviess County Employee Handbook.”

ARTICLE X – QUESTIONS

Any questions regarding this policy should be directed to the user’s respective department head.