

Wise County Computer Operations Policy

Purpose

The purpose of this policy is to implement guidelines and policies for the use of the Wise County computer systems and networks and external connections, including Internet, E-Mail, and specialized departmental access.

Policy

Wise County employees will be guided by the procedures in this policy to assure that computers and computer system are being utilized in a manner consistent with local, state, and federal laws and to ensure that information obtained from the system and placed onto the system is consistent with the goals and objectives of the county.

.01 OVERVIEW

- A. "Computer systems" consists of multiple servers interconnected into a network of workstations via hard-wire and wireless access points. Departments may have stand-alone servers and private networks connected to other departments, or may be interconnected and have varying levels of access dependant on individual department head desires.
- B. Workstations are computers that are used to access the information on the servers.

.02 RESPONSIBILITY:

- A. The Department of Information Resources (DIR) maintains complete control over the systems and is responsible for the overall administration, management and maintenance of the county's computer network.
 - 1. The DIR shall be responsible for the maintenance and upgrading of the county's various computer equipment and related peripherals, including the following.
 - a. Computer System;
 - b. Workstation and Laptop Computers;
 - c. Computer Hardware, Software, and other Peripherals;
 - d. Computer Equipment linked to the State and other agencies.

.03 MAINTENANCE:

- A. **Maintenance:** Under no circumstances shall unauthorized employees or outside individuals attempt to perform maintenance on any of the county's computer equipment (County, State, and/or Department equipment), without notification to or approval from the DIR.
 - 1. **Computer Printers:** This does not include the normal maintenance of computer printers due to paper jams, cleaning, changing ink or toner cartridges, etc. (the DIR is not responsible for obtaining normal consumables unless specific arrangements have been made. Personnel should requisition or obtain consumables as any other supplies.) The steps outlined on the printer or contained within a computer text or "help" file should be used. However, if the user has questions or problems that cannot be fixed, the DIR should be contacted.
- B. **Back-Ups:** The primary server clusters (courthouse and Sheriff's Office) performs multiple daily backups of the primary records database, scanned records, email database, and forms.

1. Backups are maintained for approximately two weeks before being reused. Backup of the primary records database is maintained for 90 days. Backups of Voice Recorder System are maintained for 3 years. Users are not expected nor required to perform individual workstation backups unless so desired.
 2. The DIR is responsible for assuring that the central records computer files are backed up on a daily basis on the appropriate storage media such as tapes, disks, or drives. Due to the nature of the backup and remote system integration, off-site storage of tapes or backup media is not required.
 3. Departments that do not use the primary server clusters for their data and maintain their own stand-alone server(s) are required to perform as a minimum weekly backups (i.e., "local backups"). A copy of the backup should be retained at the Treasurer's Office and the tape or media may be recycled every week. Departments may elect to perform backups more often; contact the DIR for an evaluation and configuration of appropriate backup systems and schedules for departments not using the SO or Courthouse server clusters. The DIR maintains a list of departments that should perform local backups.
 4. All data on any storage media not utilized as a back-up any longer due to its condition or being damaged will be given to the DIR who will assure that any data is made non-retrievable before the storage media is discarded.
- C. **Hang-Ups or Crashes:** The policy does not also include normal "hang-ups" or "crashes" of the operating system or software. Workstations computers will be shut down utilizing the "Control," "Alt," and "Delete" keys or will be shut down using the off button located on the tower or case (push and hold for up to 10 seconds). If users have any questions regarding the process or the problem is not corrected automatically, DIR should be contacted. Note: Certain types of malware require an immediate power termination using the surge protector or power cord. If malware "pops up", contact the DIR for appropriate procedures.
- D. **Periodic Purging of Temporary Files/Emptying Recycle Bin:** The policy also does not include the normal maintenance of purging temporary files, temporary Internet files, and emptying the Recycle Bin. These files cause unnecessary usage of disk space and should be periodically purged. If users have any questions regarding the procedures, the DIR should be contacted.

.04 NOTIFICATIONS OF COMPUTER-RELATED PROBLEMS:

- A. If a computer-related problem develops, i.e., inoperable condition or shutdown, it is imperative to have the system checked and returned to normal operation as soon as possible. Computer-related problems are classified as "emergency" and "non-emergency."
1. "Emergency" is defined as an essential Department function which requires 24-hour-a-day operations. An example is the computer-aided dispatch or 911 function. Notify DIR via telephone as soon as possible.
 2. "Non emergency" is defined as a non-essential Department function which does not require 24-hour-a-day operations. An example is someone's workstation computer that goes down. Obviously there are different levels of "non emergency" requests for maintenance depending on the particular needs to access documents stored on hard drives. (Note: Within certain systems, duplicate files are normally stored on the server and can be accessed from another workstation using your own user name and password.) Notify DIR either via email (preferred) or telephone.
 - a. Non-emergency issues will be prioritized. Issues that cause a loss of work product will receive the highest priority, while replacement of working equipment or non-essential upgrades will receive the lowest priority.
- B. Upon confirmation of an "emergency" computer-related problem, the DIR Administrator will be notified immediately.

.05 COMPLIANCE AND MONITORING:

- A. The DIR has the authority to conduct random monitoring to ensure compliance with county policies regarding all electronic communications. The county reserves the right to remove a user account from the network due to violations of county policies and to restrict a user from sending e-mail.
- B. The county may employ security measures to restrict access to certain computer programs and web sites and to monitor Internet activity by employees.

.06 POLICIES ON ELECTRONIC COMMUNICATIONS/INTERNET ACCESS:

- A. Internet and e-mail services are provided for certain employees to support open communications and exchanges of information. While access to the Internet is important to advancing the work of some departments, this access is a privilege which is revocable. It is essential for all users to recognize their responsibilities for all e-mail and internet actions. Conformance with acceptable use, as expressed in this policy, is required.
- B. Internet and e-mail services provided by the county are to be used for legitimate business purposes only or as designated by the department head or designee. The county maintains the right to access, delete, review, retrieve, and/or monitor all e-mail communications and Internet addresses or downloads which are stored on county computers or any county owned device that has the capability to receive and/or store emails and access the internet.
- C. Employee electronic communications are subject to monitoring for appropriateness and to assure that e-mail communications relate to official business. Employees should not have any expectations of privacy for electronic communications.
- D. Employees are subject to discipline and/or discharge for misuse of electronic communications or Internet access.
- E. All employees who have e-mail capabilities shall periodically check their e-mail messages and shall transmit communications to other members or employees when required. The keeping of unnecessary mail files cause unnecessary usage of disk space and should be periodically be purged. If users have any questions regarding the deletion procedures, the DIR should be contacted.
- F. All electronic communications shall be civil in nature and free of profanity.

.07 USE OF THE COUNTY INTERNET CONNECTION:

- A. The County is liable for employees' use of the Internet for illegal or inappropriate purposes since the electronic address that appears will be the address belonging to the county. Therefore, employees, as agents of Wise County, shall use their access to the Internet for legitimate business purposes only unless authorized by their department head or designee for specialized investigative or criminal justice purposes. Employees are subject to the disciplinary system for any illegal or inappropriate purposes utilizing the Internet.
- B. Use of Internet resources must be used to support an employee's assigned job responsibilities and for county purposes. Users must abide by copyright, contract, and other local, state and federal laws. Users must abide by generally accepted network etiquette.
- C. Due to the potential liability involving copyright laws and possible copyright infringement in the transfer of photographic images, art, logos, reports, and other materials from the Internet, no employee will download anything to county computers via hard drives, writable drives, or floppy drives without the expressed permission of the DIR.

- D. Use of Internet resources to access, transmit, or process obscene material, inappropriate or otherwise offensive text or graphic files, or files dangerous to the integrity of the network, are prohibited, unless authorized by the Sheriff, District Attorney, or County Attorney due to on-going criminal investigations.
- E. All users should be constantly aware that confidentiality of electronic mail cannot be assured. Sensitive or confidential material is not to be sent over the Internet.
- F. Employees are restricted from using the county's Internet access for any of the following unless authorized for investigative or criminal justice purposes:
 - 1. Users intentionally representing themselves using a false identity.
 - 2. Intentionally copying any software, electronic file, program, or data without a prior, good faith determination that such copying is, in fact, permissible.
 - 3. Use for access to or distribution of indecent, obscene, or pornographic materials
 - 4. Intentionally seeking information on, obtaining copies of, or modifying files or data belonging to others without authorization of the file owner or seeking passwords of others in order to gain access to private files through the network.
 - 5. Intentionally developing programs designed to harass other users or to infiltrate a computer or computing system.
 - 6. Use of the Internet to intentionally seek out information on, obtain copies of, or modify files and other data which is private, confidential, or not open to the public inspection unless specifically authorized to do so.
 - 7. Use for private or personal business, distribution of computer games, political lobbying, and other related personal or non-Department uses.
 - 8. Other non-legitimate business purposes that violate Federal or State Law or are determined to be illegal or inappropriate.

.08 USE OF E-MAIL

- A. The county does not guarantee the privacy or security of any item stored or transmitted on its systems, and employees should not have any expectation of privacy with respect to any information transmitted or stored on any computer or computer system.
- B. The goal of the county's e-mail network is to promote teamwork, reduce paperwork, and create time efficiencies. E-mail, however, cannot replace important face-to-face meetings.
- C. To assure appropriate use of the e-mail network, employees are expected to be courteous and respect the public nature and business purposes of this communications method whether internal or external e-mail. Employees should be polite. Jokes, stories, and other inappropriate or frivolous messages, whether offensive or not, should not be sent or forwarded.
- D. The county specifically prohibits the use of e-mail in ways that may be illegal, disruptive, offensive to others, or harmful to morale such as transmission of sexual harassment or disparagement of others. Also specifically prohibited is the use of e-mail to solicit others for commercial ventures, religious, or political causes, or other non job-related solicitations.
- E. It is not acceptable to attempt to gain access to another employee's e-mail files without permission.
- F. Passwords should be protected. Employees should always log off a computer if signed on using their user name and password when they leave the area.

.09 E-MAIL ATTACHMENTS - VIRUSES:

- A. Due to the various viruses that can be attached to e-mail messages, employees are cautioned about opening any unexpected or unknown mail. The DIR will periodically update Department's computers with anti-virus program upgrades; however, it is up to employees to be aware of the media's coverage of current viruses before opening any e-mail messages sent to them.

.10 GENERAL SOFTWARE GUIDELINES:

- A. Under no circumstances shall anyone outside the DIR attempt to:
 - 1. Install new licensed software on county computers
 - 2. Re-install current licensed software on county computers
 - 3. Alter or delete licensed software on county computers
 - 4. Install upgrades to licensed software on county computers
 - 5. Install trial or demonstration versions of software on county computers
 - 6. Install software licensed to another user or computer on county computers
 - 7. Install shareware on county computers
 - 8. Copy county licensed software to use for personal use or by others
 - 9. Install county licensed software on non-county computers
 - 10. Keep any trial versions of software on county computers after the review period.
 - 11. Keep any demonstration versions of software beyond the time limit outlined by the software company in documentation.
 - 12. Keep any shareware on county computers, which may need to be purchased by a certain time limit.
 - 13. Bring copies of files from outside of the county to run or copy to drives on county computers, which have not been checked for viruses.
 - 14. Open or store downloaded files from e-mails or the Internet, which have not been checked for viruses.
- B. Employees are reminded to periodically save files they are working on during the course of their workday on computers in order to eliminate the need to redo information if the computer shuts down unexpectedly.
- C. Employees are reminded to periodically purge temporary files/empty recycle bin as outlined as preventative maintenance and keeping adequate available disk space.
- D. The introduction of outside computer software and disks into county computers or workstations could result in virus infections of the host system. Employees should inspect all disks or software for virus infection prior to introduction in the county's computer system or stand-alone computers, laptops, and notebooks.

.11 DEVELOPMENT OF DEPARTMENT SOFTWARE OR COMPUTER INFORMATION:

- A. All software developed by employees for the county's use is the property of Wise County.
- B. Said employees shall not have any claims to the property of the software nor shall it be duplicated for personal use or for selling purposes.
- C. Copies of the developed software shall not leave the premises of the county unless authorized by the DIR.

.12 INFORMATION STORED ON COUNTY COMPUTERS:

- A. All information generated, stored, or maintained by employees within the various department computers for Department purposes is the property of Wise County.
- B. Employees shall not have any claims to the confidential stored information, nor shall it be duplicated or printed for personal use.
- C. Copies of the information shall not leave the premises unless authorized by the department head or the DIR.

.13 TRIAL VERSIONS OF SOFTWARE:

- A. Employees may wish to test trial versions of certain software before making recommendations for county purchase. The DIR must be notified with the following information:
 - 1. Vendor's Name, Address, and Telephone Number
 - 2. Quantity, Description, and Cost of Item;
 - 3. The words "Trial Offer";
 - 4. Listing the time frame allowed for the trial; i.e., 30 days.
 - 5. Any additional information may be attached to further explain the product.
- B. The DIR will determine the compatibility of the software and order the software if approved.
- C. Once the trial version is received, the DIR will either install the software or allow the user to install it. The DIR will maintain the packing slip, and invoice until the user completes the review.
- D. The user is responsible for reviewing the program and reporting back to the DIR with any comments within the specified trial period.
- E. It is the responsibility of the user to delete the trial version of the software immediately after the review. If the user does not know how to perform this action, the DIR will be contacted. At no time will any trial software be left on county computers beyond the trial period specified by the appropriate software companies, and it will be the responsibility of the users to conduct their reviews prior to the time periods and to delete same. This will alleviate any liability issues for the county as well as virus infections as some software builds in viruses to activate beyond the trial period date.
- F. The DIR, after notification by the user, will either take the necessary steps to purchase the software or to return it to the vendor if applicable.

.14 PURCHASING HARDWARE AND SOFTWARE:

- A. Employees and departments may need additional hardware and software in order to complete their Department's tasks and responsibilities.

- B. The Department head or employee should discuss the need with the DIR.
- C. The DIR will conduct the research into the cost and compatibility of the hardware and/or software.
- D. If a specific vendor is known for a specialized product not available through normal purchasing channels, the DIR must be notified with the following information:
 - 1. Vendor's Name, Address, and Telephone Number
 - 2. Quantity, Description, and Cost of Item;
 - 3. Any additional information may be attached to further explain the product.
- E. The DIR will report back to the department head with the cost and compatibility issues and recommend purchase or give reasons why not to purchase. If authorized by the Department Head, DIR will purchase the product and upon receipt, install it at the departments' location as specified by the Department Head.
- F. Departments shall not purchase any hardware or software for installation on county computers or networks. All purchases of computer related hardware and software must be made by the DIR.

.15 PASSWORDS:

- A. The DIR will conduct an annual audit of the central records computer system for verification of all passwords, access codes, or access violations to maintain the integrity of the system and security of records contained in the system.
- B. For security reasons, once employees/members have completed using a computer, they are required to log out if access was gained using their user name and password.

.16 GENERAL PROHIBITED CONDUCT:

- A. Use of County Computers: Use of the county's computers is limited to purposes directly related to the mission or intent of the county.
- B. Employees will not use county equipment for personal use unless authorized.
- C. Employees will not use county equipment for any other reason except in the direct performance of their assigned duties and responsibilities or as directed by their department head.
- D. No employee shall use county computers to develop software not to be used by the county.
- E. No employee shall store personal files on county computers unless authorized by their department head.
- F. Unauthorized Access: Intentionally seeking passwords of others in order to gain access through the network to private files is prohibited.
- G. Introducing Viruses: Employees shall not purposely interrupt or disrupt the county's networks, computer services/equipment by introducing viruses. It is the responsibility of all employees to check all information transferred from any diskette into any county computer for computer viruses.
- H. Altering Software Components/Personalizing Computers: Employees shall not purposely interrupt or disrupt the county's networks, computer services/equipment by intentionally altering or damaging any software components. County computers are standardized, and employees shall not rearrange file structures without the authorization of the DIR.

- I. Downloading Current Versions of County Software: Employees shall not download more current versions of Department software unless authorized by the DIR. In many instances, compatibility issues may exist with other software releases.
- J. Computer Games or Non Work-Related Matters: Unless authorized by the department head, employees will not use computer equipment to play games or use computer resources for other than work-related activities.
- K. Use of Encryption Programs: Employees will not use any encryption program(s) without the authority of the DIR.
- L. Use of County Computer Supplies for Personal Use: Employees shall not procure county computer supplies for personal use.
- M. Copying or Installing County Software: Most software is protected by copyright laws. Therefore, employees will not copy or transfer any county programs for any unauthorized use. Employees shall also not copy, transfer, or install any programs or files onto county computers without the authorization of the DIR.
- N. Lending or Borrowing Software: Employees will not give, lend, or sell copies of county-owned software to others unless the original software is clearly identified as shareware or in public domain and with the authorization of the DIR.
- O. Pirated or Illegal Software: Employees will not download or upload pirated or illegal software.
- P. Dissemination of Confidential and/or Sensitive Information: Employees will not disseminate any confidential or sensitive information via e-mail or over the Internet to an unsecured site. (NOTE: Messages on e-mail are often considered public records and must be produced if required by law or court order.)
- Q. County Information Stored on County Computers: No information stored on County computers shall be copied, transferred, forwarded, or e-mailed for personal use or to be used by others unless authorized by the department head or the DIR.
- R. Development of any County Software: Employees who develop any software on county time for the county's use is the property of Wise County. Said employees shall not have any claims to the property or the software nor shall it be duplicated for personal use for selling purposes. Copies of the developed software shall not leave the premises unless authorized by the DIR.
- S. Electronic Mail Polices: Unless involved in a legitimate criminal investigation, employees will not utilize county computers to:
 - 1. Threaten, intimidate, disturb, or harass other users by sending unwanted files or mail. All communications will conform to the policies as set forth in the Policies and Procedures Manual.
 - 2. Send images that contain nudity, or send images or words of an offensive or suggestive nature, or anything that can be construed against the County's sexual harassment policy.
 - 3. Send jokes or comments that disparage a person or group because of race, ethnic background, national origin, religion, gender, sexual orientation, age, verbal accent, source of income, physical appearance or agility, mental or physical disability or occupation.
- T. Internet Prohibitions: Unless involved in a legitimate criminal investigation, employees will not utilize County computers to:
 - 1. Access pornographic or other deviant web sites;

2. Download any information from the Internet for County or personal use without the prior approval from the DIR;
3. Use the Internet for financial gain, for any commercial or illegal activities, or for political lobbying.

APPENDIX A

BACKUP DISTRIBUTION (as of March 2011)

DEPARTMENTS REQUIRED TO PERFORM LOCAL BACKUPS

Departments required to perform local backups assure the integrity of their working data in case of a catastrophic failure of equipment or a natural disaster. As a minimum, weekly backups stored off-site are required, though daily backups are preferred.

- Financial Building (Auditor and Treasurer's Office)
- Developmental Building (Public Works, 911 Addressing)
- Tax Assessor/Collector
- Asset Management
- Veteran's Administration
- Juvenile Probation
- Elections Administration
- AgriLife

DEPARTMENTS RECOMMENDED TO PERFORM LOCAL BACKUPS

The following departments maintain their primary records on a web-based system or use the county cluster system but still have a local server. Local backups are not required, but recommended for locally stored forms, specialized data, emails, etc. Recommended local backups may be stored off-site but it is not required.

- Justice of the Peace, all precincts
- Public Works (old building, if picture data needed)
- Indigent Health Care/EMS Administration
- Animal Control
- County Clerk

STAND-ALONE SYSTEMS

Stand alone individual computers or very small networks may perform individual workstation backups as desired to protect their stored forms and any stored emails. Examples of stand-alone systems:

- Commissioner Precinct Offices
- County Engineer
- EMS Stations (Medic 1, 2, and 3)
- Project Management
- Public Works (Annex)