

A MESSAGE FROM THE BOARD OF ADA COUNTY COMMISSIONERS:

Information serves as the foundation for all Ada County operations. Applying the correct methodologies and policies to our computer information systems is critical in efficiently and consistently serving the taxpayer.

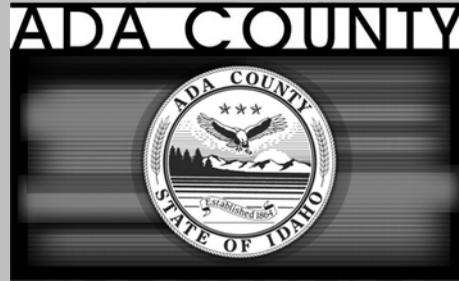
Most County positions require the use of computers and access to our information systems. It is important for everyone to fully understand the responsibilities which accompany the use of these systems.

Every employee is required to read and understand the contents of this publication which is a condensed version of the Ada County Computer Information Policy Statement. The full text is available from your department head or elected official.

We want to emphasize the critical nature of our computer policies, especially:

- All hardware, software, e-mail and Internet access provided by Ada County is to be used for the purpose of facilitating the work of the County and its agencies.
- Employees have no right to privacy with regard to their use of the County's computers and computer systems, including use of e-mail and the Internet.
- Internet use and e-mail communications may be monitored.
- Ada County does not condone the illegal duplication of software.
- The user-id/password combination is the cornerstone of Ada County computer security. All provisions for password control will be observed.

All Ada County employees are responsible for protecting Ada County's information assets.



Computer Policy Statement

Ada County
Information Technology
200 West Front Street
Boise, Idaho 83702
(208) 287-7020

V2.1
July 1, 2006

E-MAIL

Use of e-mail on Ada County computers is to promote internal business-related communications between employees. The computers belong to the County and are provided to employees for the purpose of facilitating the work of the County and its agencies. Employees have no right to privacy with regard to their use of the County computer system and computers including the use of e-mail and internet. The County does not waive any privileges, including those provided by statute, rule or common law. Passwords are not indicative of privacy, rather a password is a security tool used on behalf of the County. E-mail communications can and may be monitored. Therefore, the County encourages its employees to refrain from using the County computer system for transmission of personal information and communications.

Appropriate usage of e-mail is internal business-related communications. Prohibited usage includes, but is not limited to, distribution of chain letters, inappropriate humor, offensive graphics and images or language that may offend someone on the basis of age, race, sex, religion, national origin or disability.

E-mail may be monitored for personnel purposes in order to prevent inappropriate and/or unprofessional comments or activities over the County's e-mail system. E-mail and electronic data may also be accessed for other work-related reasons.

All employees are prohibited from transmitting over the Internet any County information and/or electronic data that is regarded as privileged or confidential without first securing a method of scrambling (encryption) the transmission from IT. If there is a doubt as to whether information is privileged or confidential or as to whether a transmission will utilize the Internet, employees are required to discuss the issue with their supervisor before transmitting.

INTERNET USE

Internet access on Ada County computers is a privilege extended to some of the County's employees. Proper usage of the Internet is the responsibility of each Ada County employee. Use of the Internet on County computers is provided to employees for the purpose of facilitating the work of the County and its agencies and only by the authorization of an elected official or department head.

Internet communications can and may be monitored. Internet communications may be monitored for personnel purposes in order to prevent inappropriate and/or unprofessional activities over the County's Internet.

Internet communications and electronic data may also be accessed for other work-related reasons. Employees have no right to privacy with regard to their use of the Internet on County computers.

Employees must refrain from using County access to the Internet for non-work related purposes. Prohibited sites on the Internet include those containing offensive graphics, images, and language. Downloading of copyrighted, protected materials or software is strictly prohibited.

Internet e-mail shall not be used for non-work related purposes. Prohibited uses of Internet e-mail include but are not limited to the distribution of chain letters, inappropriate humor and offensive graphics or images, and language that may offend someone on the basis of age, race, sex, religion, national origin or disability. The Internet shall not be used to send sensitive, privileged and/or confidential information, without first securing a method of scrambling the transmission from Ada County Information Technology (IT). Also see Ada County E-Mail and Electronic Data Policy, Section C.

SOFTWARE

Ada County purchases or licenses the use of copies of computer software from a variety of outside companies. Ada County does not own the copyright to this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce the software or its related documentation for use on more than one computer.

Making additional copies or loading the software onto more than one machine may violate federal copyright law and be considered piracy.

Ada County employees learning of any misuse of software or related documentation within the County shall notify the department manager, Ada County Information Technology or the Ada County Civil Prosecutor's Office.

According to United States Copyright Law, illegal reproduction of software can be subject to civil damages of as much as One Hundred Thousand Dollars (\$100,000.00) per work copied, and criminal penalties, including fines and imprisonment. Ada 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. Ada County does not condone the illegal duplication of software.

Shareware and freeware is not allowed on Ada County computers as it is difficult to track and ensure license compliance with such applications. Installation or use of any games is prohibited on Ada County computers.

Personal Music in the form of MP3, WMA or other electronic music media are not to be stored on the Ada County Network.

All software installation will be done under the supervision of the Ada County Information Technology Department.

Many times software is loaded on a computer, "inherited" from another user, applications are brought from home and loaded onto an office computer, programs are "passed around" the office and software is often downloaded from bulletin board services. All are potential illegal copies of the software. It is Ada County's policy that an Ada County Software Security Officer will conduct random Ada County audits to verify that every application used within Ada County is a legal copy. Any programs that are not legal must and will be removed from the system.

HARDWARE

Ada County has several objectives in mind when acquiring computer hardware. A significant goal is to reduce incompatibility problems. Others include, reducing administrative costs associated with the acquisition of microcomputer products, reducing implementation time and complexity, improving management and control, improving quality and reliability of purchases, reducing support confusion, and improving the budget planning process.

The focus on compatible hardware is due to the fact that compatible hardware significantly reduces the cost of the Ada County maintenance contract, ensures compatibility and consistency in the way Ada County operates software and connects to the network, and reduces the complexity of managing multiple manufacturer's products from across the enterprise.

All computer hardware installation will be done by the Ada County Information Technology Department.

SECURITY

Computer information security is the responsibility of each Ada County Employee. Computer information security is the protection of information assets from accidental or intentional, but unauthorized, disclosure, modification or destruction including temporary unavailability.

Information asset refers to computer hardware and/or software owned, leased, managed, or used by Ada County. All application software, information in databases or files, information in handwritten, typed, pictorial, digital or analog form, operating system software, utility programs, printouts, storage media and their contents, terminals, data communication devices and computers constitute Ada County's information assets. A particular information asset may refer to one or many of the items listed.

The objective of this policy is to insure the safeguard of all Ada County data assets.

All Ada County employees are responsible for protecting Ada County's information assets. Ada County employees learning of any breach of information security within Ada County shall immediately notify their respective elected official or department head, Ada County Information Technology Department or the Ada County Prosecutor's Office, Civil Division. Ada County employees are required to comply with all information security policies.

DATA ACCESS

To insure maximum information security, Ada County administers computer security under the program of "least possible privilege to perform position." Each user will be given the rights to access only the information necessary to perform the duties of their position. Each computer device must have its own device ID.

All data residing on Ada County systems is the property of Ada County and its representatives and is to be used by and for Ada County for county purposes only. Under no circumstances is Ada County data to be viewed, downloaded, copied, or distributed without the express written consent of the data creator/owner or elected official or their designated department head.

All computers must be turned-off at night or when left unattended for an extended period of time. Prior to turning-off a computer, all applications and the operating system will be shut down according to the guidelines published by the software manufacturer.

PASSWORD CONTROL

Password Control -Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system. Therefore, under no circumstances are ID's and passwords to be shared, (this is inclusive of an employee's supervisor and IT personnel), or written down and placed in a visible location on or around the computer or desk.

- ❑ All passwords, (AS/400, network and mail), must be changed every 120 days. Individual users can have the same password for their AS/400, network and mail accounts.
- ❑ Passwords must be at least 5 characters in length but no longer than 10 characters. There are no limitations to the characters that can be used in the password. They can be composed of any characters on the keyboard.
- ❑ Passwords cannot have adjacent digits in a password. This is to prevent a password being a numeric string such as '12345' or '11111'.
- ❑ The number of times a character can appear in the password is limited.
- ❑ Characters can appear more than once in a password as long as they were not used consecutively. This is to prevent a password value of something similar to 'aaaaa' or 'bbbbb'.
- ❑ A character can not occupy the same space in the new password as it occupied in the old password. This is to eliminate passwords like 'mike1' and 'mike2'.
- ❑ A user can not use the same password for 18 changes. This was put into place to prevent the use of the same two passwords over and over.

DATA STORAGE

Network computers will be configured to store all data files on assigned network drives. All network servers are backed-up each night. If an individual hard drive malfunctions, program files can be recreated from the manufacturer's disks and data files which are stored on the assigned network drives can be recovered. If an individual hard drive malfunctions, the data is lost and cannot be recovered. Personal music found on the network will be deleted immediately and is not retrievable.

RECORDS RETENTION

DATA DISPOSAL

All data at Ada County is treated as confidential for County purposes, even after it seems to be no longer useful to Ada County. Therefore, disposal of data or data storage media is handled in a secure manner. Disk drives, diskettes, tape reels and cartridges and other such media must be erased before they are transferred to new ownership (inside or outside Ada County).

If they are being disposed of they must be erased or otherwise damaged such that their contents are rendered unreadable. The largest opportunity for information leakage occurs in the disposal of printed reports. Particularly because Ada County is recycling a large volume of paper, care must be taken to render unreadable any report or document that carries a Moderate or High risk. (Remember that disposal of any document at Ada County is subject to rules governing County records retention. Before disposal, please contact the Ada County Clerk's Office.)

COMPUTER VIRUS DETECTION

All Systems (defined as desktop computers, laptop computers, servers, or any other type of personal/corporate system) connecting to the Ada County Network shall meet the following requirements:

1. Have an anti virus program installed and up to date.
2. Have all current security and operating system patches installed.

Systems that do not meet these criteria may be automatically re-directed into a "quarantine" Vlan and given the option of installing the required software and patches. If the user chooses not to install the required software they may be unable to connect to any Ada County Network resources.

Any Removable storage device (defined as USB hard drives, thumb drives, flash drives, or any other type of data capable device) that has been used on a computer system outside of the Ada County Network must be checked for viruses by the user before being used on a workstation or server on the Ada County Network.

NON-COMPLIANCE

All policies are in full force and effect both during and after working hours. Non-compliance with these policies may result in formal disciplinary proceedings or the permanent cancellation of computer privileges. Any employee who violates these policies may be subject to dismissal, suspension, demotion or other adverse action.

DEVIATION

There shall be absolutely no deviation from this policy without the written authorization from Information Technology Executive Committee. Any deviation without said written authorization shall be considered non-compliance.

EMPLOYEE SIGNATURE STATEMENT

All employees will read and sign an Ada County Computer Policy Statement before being given computer access privileges.