

# **ADA COUNTY INFORMATION TECHNOLOGY POLICY STATEMENT**

The purpose of this policy statement is to set forth Ada County's policy regarding hardware and software purchasing, software licensing, Internet usage, E-mail usage and security.

## **I.**

### **SOFTWARE PURCHASING AND LICENSING POLICY**

#### **A.**

##### **Introduction**

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.

#### **B.**

##### **Objectives**

With regard to use on Ada County networks or on multiple machines, Ada County employees shall use software only in accordance with the license agreement. All software comes with a license agreement that specifically states the terms and conditions under which the software may be legally used. Licenses vary from program to program, and may authorize as few as one computer or individual to use the software, or as many as several hundred networked computers and users to share the application across a system. It is important that all licenses accompanying the application are read and understood to ensure that Ada County has sufficient legal copies of the software. Making additional copies or loading the software onto more than one machine may violate federal copyright law and be considered piracy.

#### **C.**

##### **Guidelines**

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 (\$150,000.00) 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.

The following is Ada County's policy regarding specific components of software management:

1. Software Not Authorized by Ada County - Shareware and freeware is not allowed on Ada County computers as it is difficult to ensure license compliance with such applications. Installation or use of any games is prohibited on Ada County computers. Software applications cannot be brought from home and loaded onto an Ada County computer. 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.
2. Software Acquisition Process - Because software is expensive and is a critical part of the information processing function, Ada County has developed guidelines for purchasing decisions. Each Department shall work with an Information Technology Department analyst to determine the department's needs. The Information Technology Department will then work with each department in fulfilling the specified requirements. Software packages may be evaluated by department heads to determine which is best for the specific department, if such evaluation is allowed by the publisher. All copies of the software will be removed from the computer and related magnetic media within the specified time limitations. Software purchases for each department will be budgeted for annually out of each department's budget. All software purchases will then go through each department's standard purchasing procedure, the software license will be kept on file with the Information Technology Department.

Installation - All software installation will be done under the supervision of the Ada County Information Technology Department. This is to aid in the elimination of problems associated with printer set-up, software and hardware compatibility and correct application of system defaults. A department may choose to have one of its own employees install software, provided the employee has been trained and/or certified by the Ada County Information Technology Department, consults with the Ada County Information Technology Department prior to all software installation and follows all licensing and inventory requirements. An inventory of all software in use by the County is kept by the Ada County Auditor's Office and the Ada County Information Technology Department. This includes software installed on computers which are not owned by Ada County, however which are solely used by Ada County employees, as is the case in our court systems. The inventory system is necessary to maintain software and hardware maintenance contracts, document and track Ada County assets and ensure that all installed software represents a licensed copy which has been purchased by Ada County.

3. Home Use - On an as-needed basis, software license agreements will be reviewed to determine if copies of software purchased for Ada County-owned computers may also be installed on an individual's home computer for non-concurrent use. If the license permits

home use, the employee must follow the sign-out form and procedure to ensure that all software and technical documentation loaned out is returned to Ada County and that all software is removed from the employee's machine when its use is no longer required by the department or upon the cessation of an employment relationship with Ada County. If such uses are prohibited, purchasing of additional copies of the software may be considered by the department head of the department in which the person is employed.

4. Software Audits - The Information Technology Department will conduct a Software Audit no less than once every other year; a report will be given to the department head showing the number of licenses and the number of users. The report is intended to present the knowledge of how many legal licenses are installed within each department.
5. Virus Check - 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.

The media of all new software must be checked for viruses before being used or installed on a workstation or server on the Ada County Network.

The hard disk of a stand-alone system must be checked for viruses by the Information Technology Support Technician prior to the system being connected to the Ada County Network.

A stand alone computer system with virus detection software will be available for checking Removable Storage devices.

## II.

### HARDWARE PURCHASING POLICY

#### A.

##### Introduction

Ada County purchases computer hardware from a variety of outside companies. The Information Technology Department continually monitors and reviews the computer industry and the tools of Information Technology, always mindful of the County's need for products capable of high performance, reliability and compatibility.

#### B.

##### Objectives

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.

#### C.

##### Guidelines

Hardware Acquisition Process - Because hardware is expensive to purchase and maintain, and is a critical part of the information processing function, Ada County has developed guidelines for hardware purchasing decisions. It is absolutely critical that Ada County maintain a homogenous microcomputer hardware base by limiting the types of microcomputers purchased to those that have been tested and are known by the Information Technology Department to be reliable, work well together when networked and are easily serviceable. By doing this the functionality at the desktop and network level is improved and total cost of ownership (TCO) is reduced.

Each Department shall work with their Information Technology Department analyst to determine the department's needs. The Information Technology Department's technology purchasing specialist will then work with each department in fulfilling the specific requirements. All hardware purchases for each department will be budgeted for annually out of each department's budget and will be purchased through each department's standard purchasing procedure.

All computers and related hardware purchased by Ada County departments must follow the guidelines set forth by Information Technology each year during the budget process. It is important that Ada County acquire computers known to function reliably, be readily serviceable, be totally compatible with our network and software and have a reasonable life expectancy. To ensure Ada County meets these microcomputer purchasing goals, it is critical that only “first” or “second tier”, “business-grade” microcomputers are acquired.

Installation - All computer hardware installation will be done by the Ada County Information Technology Department. An inventory of all hardware in use by Ada County is kept by the Ada County Auditor’s Office and the Ada County Information Technology Department. This inventory system is necessary to maintain software and hardware maintenance contracts and document and track Ada County assets.

**D.**

**Ada County Purchasing Procedures**

[http://ln1/WEB/ADAWEB.NSF/a452421cb76b9d2c87256743006b000c/386489531cf6f78e87256cf70056ad17/\\$FILE/2005%20Bid%20Manual.pdf](http://ln1/WEB/ADAWEB.NSF/a452421cb76b9d2c87256743006b000c/386489531cf6f78e87256cf70056ad17/$FILE/2005%20Bid%20Manual.pdf)

**III.**

**COMPUTER INFORMATION TECHNOLOGY SECURITY POLICY**

**A.**

**Introduction**

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.

**B.**

**Objectives**

The objective of this policy is to insure the safeguard of all Ada County data assets. This policy will define information security, classification of data assets, who is responsible for the Ada County data assets and the consequences of non-compliance.

## C.

### Guidelines

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.

1. Ownership And Individual Responsibility - The accountability principle requires that there be a single point of responsibility for an asset. Therefore, Ada County requires that all information assets have an Owner and this Owner becomes responsible for the information asset, including being the designated "custodian" for public records purposes, as defined by Idaho Code section 9-337. In the absence of other ownership assignments, information assets used exclusively by a single person are considered to be owned by that individual.

Owner - Information asset owner (Owner) is the person, group, or other entity which is charged with maintaining an information asset on behalf of Ada County. Determination of ownership of an information asset shared by more than one person may be difficult because ownership is dependent upon several factors. When these factors are arranged hierarchically, the Owner may be determined using a "best fit" criteria.

- Federal laws, State statutes, or County Policy which designate a department or individual as having the responsibility for an information asset constitute the highest ownership criteria.
- An administrative directive that specifies a person or group's information asset responsibilities is justification for ownership in the absence of any higher level of responsibility within Ada County.
- Data created or collected by a person or group is owned by that person or group in the absence of any higher level of responsibility within Ada County. If more than a single County department is involved in the creation or collection, the department most at risk in a case of loss of the asset is the owner in the absence of any higher level of responsibility within Ada County. In this case departments must come to written agreement regarding information asset ownership.
- An information asset may be utilized by a person or group which is not directly an Ada County department. In this case the person or group using the asset views itself as a Custodian for the Owner who supplied the information asset, in the absence of any higher level of responsibility within Ada County.

The Owner is charged with the following responsibilities on behalf of Ada County:

- Ensuring that release of the information asset complies with applicable laws, ordinances, and administrative policies;
- Authorizing access to, custody of, and release of the information asset;
- Judging the value and importance of the information asset in order to assess the optimal degree of security to apply to it;
- Maintaining or delegating to appropriate individuals or groups the responsibility for maintaining security for the information asset;
- Specifying the security requirements to apply to the information asset and accepting responsibility for violations above that level of security; and
- Dissemination of the information asset.

Ownership of data may be transferred at any time by formal written consent of all parties involved, so long as such transfer does not conflict with directives stated in any law, statute, charter, ordinance or directive.

User - Information asset user is the person, group, or other entity that has been authorized to use the information asset by the Owner. Users must comply with all security directives of the information asset as specified by the Owner, Ada County Information Technology, (IT), and/or by the Ada County Computer Information Security Policy. Users are responsible for an information asset to the extent that they are authorized to use the asset. (For example, if an Owner requires the use of passwords, a User is responsible for proper use of the password. If the asset was compromised as a result of misuse of the password, the User would be responsible. If the Owner had not required passwords and an asset was compromised as a result, the Owner would be responsible.)

Security Officer - Information asset security officer means the individual(s) in IT, who is/are responsible for overall systems security, maintaining systems administration security passwords, advising Owners on appropriate security measures and confirming that information asset security is maintained at the level specified by the Owner, IT, and/or by the Ada County Information Technology Security Policy. The Security Officer may offer recommendations to Owners regarding information asset security and has the option to set higher security levels than requested by the Owner if the lower security levels may compromise overall system security. They are responsible for monitoring compliance and reviewing security decisions and for reporting security problems to the Owner and/or the IT Director. The Security Officer position/responsibility is exclusive to IT personnel.

2. Classification of Information - Information assets may be violated intentionally or accidentally. Each information asset has a risk associated with it in terms of the cost to Ada County if that asset is rendered unavailable or is improperly exposed. For every risk there is at least one control to neutralize it. However, some of these controls may be too expensive to implement in relation to the information asset involved. Therefore Ada County applies controls in relative proportion to the value of the asset being protected. Rather than specifying specific controls for every asset, a general risk classification is assigned which encompasses a base level of control. This assignment may be made on specific assets or on an entire system, in which case all information assets comprising the

system carry that as a base risk classification. (Note that this methodology does not preclude the Owner from specifying additional security controls.) Benchmarks for identifying risk classifications are identified in this section.

In the course of developing and maintaining an information asset, potential risks to the asset are identified, the costs associated with each risk estimated (in terms of costs to Ada County or characteristics of each risk category), and a risk classification assigned. This process occurs initially as part of any new system proposal (since security adds costs to any system) by the system designer or design team. The Owner considers this proposal and may consult with the Security Officer. The Owner then assigns the risk classification. The classification may be updated throughout the life of the system by the Owner to reflect changing needs and conditions. The Security Officer may be asked to assist in reevaluations. Each risk classification specifies minimum control levels that will be applied to the information asset. Note that assets used by more than one system must meet the security of the system at highest risk. Also note that the Owner is responsible for violations that occur at risk levels higher than those specified (for instance, if the Owner specified a low risk and a security breach occurred that could have been prevented by specifying a Moderate risk, the Owner assumes responsibility for the consequences of the security breach).

Exception to rules and procedures have probably caused the failure of more safeguards than any other problem. Ada County's information assets adhere to the control levels specified with this exception: The Owner may deviate from these security requirements and accept an identified risk only when it has been clearly demonstrated that available options for achieving compliance will have a significant and unacceptable operations impact. The Owner accepts all responsibility for violations occurring as a result of this risk acceptance. Risk acceptance involving confidential information assets or critical information assets (those whose loss or public display would be seriously damaging to Ada County) must be approved by the Owner and communicated to and approved by the Board of County Commissioners who then accept the responsibility for violations occurring as a result of this risk acceptance.

Low Risk - Information assets identified as low risk have one or more of the following characteristics:

- Transitory in nature (an informational e-mail message which would be deleted after being read);
- Easily and inexpensively reproduced (reprinting an existing report);
- Of little or no value outside of County government; or
- Valued at up to \$100.

All County information assets are assigned at least a low risk classification.

Moderate Risk - Information assets identified as moderate risk have one or more of the following characteristics:

- Shared by more than a single person;
- Would take more than one person-day to reproduce, or cannot be repurchased within current budget limitations;
- Of informational value outside of County government; or
- Valued at between \$100 and \$1000.

Most County information assets are assigned a moderate risk classification.

High Risk - Information assets identified as high risk have one or more of the following characteristics:

- Required specific budgetary approval for purchase;
- Potentially damaging to Ada County if exposed;
- Is practically impossible to reproduce or repurchase and is still viable to Ada County;
- Would halt work of two or more County employees if compromised; or
- Valued at more than \$1000.

3. Physical Access - Access to the main computer room is restricted to personnel working on the shift to which they are assigned and to escorted, authorized visitors.

With the proliferation of personal computers, special attention must be paid not only to protecting the information by locking it up when not in use, but protecting the microcomputers from theft as well. These threats are combined when data is stored on "non-removable" medium (hard disk), since the data is stolen as a result of the theft of the device itself.

4. 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 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. All terminals must be signed-off at night or when left unattended for an extended period of time.

For the purpose of this document the term "data" shall represent any and all files (spreadsheet, document, image, txt, etc.) that are stored either on shared network resources and/or local storage. Storage shall include both fixed devices and removable media. The term "email" shall represent any and all electronic communication initiated and/or received by Ada County systems.

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.

Likewise, all email communication initiated and/or received by Ada County systems is the property of Ada County and its representatives and is to be used by and for Ada County purposes only. Under no circumstances is any email to be read, intercepted, or re-directed without the express written consent of the email creator/owner or elected official or their designated department head.

5. 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 'bbbbbb'.
  - 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.
  
7. 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.

8. Dial-Up Control - All dial-in access to all Ada County computer systems must be equipped with and use dial-back security controls or Ada County Security Dynamics Secure Identification System. Dial-back facilities provide protection from many of the risks by requiring pre-identification to access the system prior to logon. The incoming call is received, authenticated, and then disconnected. The dial-back device then initiates the connection to the authorized remote location. Dial-in telephone numbers are not to be published or posted.

No dial-in telecommunication line/modem shall be attached to any computer or terminal without prior approval from IT. Computers attached to the Ada County network cannot have modems attached to a line with call receiving capacity or software programs such as "PC Anywhere" and "Carbon Copy."

9. Attachment To The Ada County Network By Outside Agencies - All connections to public or unsecured networks, such as the Internet, must have firewall protection.

Any outside agency wishing to directly attach to the Ada County network must have a contract signed by The Board of Ada County Commissioners and the "Owner" of the data to be accessed. Prior to making a direct network attachment, the requesting agency must agree to conform to the Ada County Security Policy. Ada County will have the right to a computer systems security audit to be completed on the requesting agency. Ada County reserves the right to deny any application for direct connection to the Ada County network.

Ada County further reserves the absolute right to terminate the agency's attachment for any reason. No property right is received when attachment is allowed. It is merely a revocable privilege.

10. 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.)

11. Computer Virus Detection - County employees will report all instances of computer virus to IT immediately. Anti-virus software will be installed on all microcomputers to detect, identify, isolate, and eradicate viruses. This software will be updated frequently to fight new viruses. In order that the viruses are intercepted as early as possible, the software will be kept active on a system, not used intermittently at the discretion of users.

Any computer which is identified as containing a computer virus will have correctional measures taken immediately. This includes virus checking all floppy disks used by the infected computer, all computers which may have shared portable magnetic media with the infected computer and all portable magnetic media suspected of being used in the infected computer.

12. Personnel - In multi-user computer environments, additional investigation into the background of users is warranted. Employment and character references offered by applicants must be studied. Although this will not necessarily screen applicants for honesty or integrity, it may flag areas that need additional investigation. For information assets designated High risk, credit references can indicate financial habits which in turn can be an indication of willingness to assume responsibility for one's own actions.

Criminal background investigations will be conducted on all candidates considered for a position of trust and be completed before the employee is placed in the sensitive position. An example of such a position is IT personnel.

Upon change of status or termination of employment, the employee's supervisor, (or former supervisor), is responsible for notifying the IT Security Officer of the change and to collect County information assets that may have been issued to the employee. IT personnel are then responsible for disabling or revising any accounts used by the former employee. If the employee was an information asset owner, the supervisor may designate a Custodian for the asset until the vacancy is filled.

#### IV.

### **E-MAIL AND ELECTRONIC DATA POLICY**

#### A.

##### **Purpose**

The purpose of this policy is to explain the proper use of e-mail and electronic data. Use of e-mail on Ada County computers is to promote internal business-related communications between employees. The County has the same interest with regard to electronic data and e-mail generated by employees as it has with regard to paperwork.

The computers belong to the County and are provided to employees for the sole 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.

#### B.

##### **Appropriate Usage**

Appropriate usage of e-mail is internal business-related communications. Employees are prohibited from using e-mail for non-work related purposes. 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.

#### C.

##### **Monitoring**

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.

**D.**

**Internet Transmission of E-Mail or Electronic Data**

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.

V.

**INTERNET POLICY**

A.

**Introduction**

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 sole purpose of facilitating the work of the County and its agencies and only by the authorization of an elected official or department head.

B.

**Privacy**

Employees have no right to privacy with regard to their use of the Internet on County computers. Internet usage will not regularly be monitored; however, it cannot be assumed that the usage is confidential.

C.

**Appropriate Usage**

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 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 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.

## **VI.**

### **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.

## **VII.**

### **DEVIATION POLICY**

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.

## **VIII.**

### **EMPLOYEE SIGNATURE STATEMENT**

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