

Canyon County IT Policy

1.0 SOFTWARE PURCHASING AND LICENSING POLICY.....	1
1.1 Introduction.....	1
1.2 Objectives.....	1
1.3 Guidelines.....	1-3
2.0 HARDWARE PURCHASING POLICY.....	4
2.1 Introduction.....	4
2.2 Objectives.....	4
2.3 Guidelines.....	4
3.0 COMPUTER INFORMATION TECHNOLOGY SECURITY POLICY.....	4
3.1 Introduction.....	4-5
3.2 Objectives.....	5
3.3 Guidelines.....	5-12
4.0 E-MAIL AND ELECTRONIC DATA POLICY.....	12
4.1 Purpose.....	12
4.2 Appropriate Usage.....	12
4.3 Monitoring.....	12
4.4 Internet Transmission E-Mail or Electronic Data.....	12
5.0 INTERNET POLICY.....	12
5.1 Introduction.....	12-13
5.2 Privacy.....	13
5.3 Appropriate usage.....	13
6.0 NON-COMPLIANCE.....	13
7.0 DEVIATION POLICY.....	13
8.0 EMPLOYEE SIGNATURE STATEMENT.....	13

CANYON COUNTY INFORMATION TECHNOLOGY (IT) POLICY STATEMENT

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

1.0 SOFTWARE PURCHASING AND LICENSING POLICY

1.1 Introduction

The County purchases or licenses the use of copies of computer software from a variety of outside companies. The County does not own the copyright to this software or its related documentation. The County only has the right to reproduce the software or related documentation as authorized by the software vendor. Canyon County does not condone the illegal duplication of software.

1.2 Objectives

With regard to use on County computers, Canyon County employees shall use software only in accordance with the terms of that software's license agreement.

1.3 Guidelines

Canyon County employees learning of any illegal use of software or related documentation within the County must immediately notify their elected official, department manager or the Canyon County Prosecutor's Office, Civil Division.

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

- A. Software Not Authorized by Canyon County - The download and installation of Shareware and freeware by county employees requires written approval from their Elected Official. Installation of any game is prohibited on County computers. Software applications cannot be brought from home and loaded onto a County computer. It is Canyon County's policy that the County may conduct random audits to verify that every application used within Canyon County is a legal copy. Any programs that are found to be illegal will immediately be removed from the system. An employee's use of unauthorized software or unapproved shareware or freeware may result in disciplinary proceedings against that employee.
- B. Software Acquisition Process - Each Office may work with an IT analyst to determine its needs. Because software is expensive and is a critical part of the information technology, each Office is encouraged to work with IT in order to ensure the success of the application specification, procurement, development, deployment, and support. The IT Department will then work with each Office in fulfilling the specified requirements. Software packages may be evaluated by Elected Officials to determine which is best for the specific Office, if such evaluation is allowed by the publisher. All copies of the evaluation software must be removed from the computer within the specified time limitations. Software purchases for each Office will be budgeted for annually out of each Office's budget. All software purchases will then go through each Office's standard purchasing procedure, the software license will be kept on file with the Information Technology Department.
- C. Installation - All software installation will be done under the direction of the Canyon County IT 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. An Office may choose to have one of its own employees install software, provided the employee has been trained and/or certified by the IT Department, consults with the IT Department prior to all software installation and follows all licensing and inventory requirements. A list of all purchased software in use by the County is kept by the Information Technology Department. The inventory system is necessary to maintain software and hardware maintenance contracts, document and track County assets and ensure that all installed software represents a licensed copy which has been purchased by Canyon County.

- D. Software Audits - The Information Technology Department shall conduct a Software Audit no less than once every other year; a report will be given to the Office 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 Office.
- E. Virus Check - All workstations, PC's, and Laptops connecting to the Canyon County Network shall meet the following requirements:
 - a. Have an anti virus program installed and up to date.
 - b. Have all current security and operating system patches installed.

Systems that do not meet these criteria may be quarantined until the required software and patches are installed. While in quarantine the system will not be able to connect to any County resources. Any removable storage device (defined as USB hard drives, thumb drives, flash drives, or any other type of data storage device) that has been used on a computer system outside of the Canyon County Network should be checked for viruses by the user before being used on a workstation or server on the County Network. The media of all new software should be checked for viruses before being used or installed on a workstation or server on the County Network. A stand alone computer system with virus detection software will be available in the IT Tech room for checking Removable Storage devices.

2.0 HARDWARE PURCHASING POLICY

2.1 Introduction

Canyon County purchases computer hardware from a variety of outside companies. The IT 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, compatibility, and return of investment.

2.2 Objectives

Canyon 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 IT hardware, reducing implementation time and complexity, improving management and control, improving quality and reliability of purchases, improving economy of scale, and improving the budget planning process which enhances the total cost of ownership.

2.3 Guidelines

Hardware Acquisition Process - Because hardware is expensive to purchase and maintain, and also performs a critical role in maintaining application availability and security, IT provides guidelines for hardware purchasing decisions. It is important that the County acquire hardware which meets our applications software requirements, is reliable, has reasonable life expectancy, is readily serviceable, is supportable and is compatible with our network and security requirements. It is also important to reduce the Total Cost of Ownership, and choose vendors which are flexible and responsive to the County's changing Business needs.

Offices planning to purchase hardware which may be connected to the County Network or eventually require IT Support, must notify IT early in the procurement process and identify a contact person. IT must then identify a Systems Analyst to fully support them. Each Office must consult with the Systems Analyst prior to purchasing *.

The Systems Analyst will collaborate with the Office's Contact person to identify and meet collective purchase objectives. All hardware purchases for each Office will be budgeted for annually out of each Office's budget.

To support efficiencies and economy of scale, County Offices are strongly encouraged to utilize IT's procurement services. The Office must obtain *, but not necessarily purchase against, a quote from IT Procurement prior to purchasing.

* In some cases, requirements to consult with a Systems Analyst or obtain a quote from IT prior to purchasing may be waived in writing by IT Senior Management. For example, it would make little sense to unbundle a computer to get a separate quote from IT, when purchasing a bundled system containing an embedded computer. Likewise, it probably would not make sense to consult with a Systems Analyst in that case.

Installation - All networked computer hardware installation should be done by the IT Department or a duly appointed representative. An Office may choose to have one of its own employees install hardware, provided the employee has been trained and/or certified and consults with the IT Department prior to all hardware installation. An inventory of networked hardware in use by Canyon County is kept by the Canyon County Auditor. This inventory system is necessary to maintain software and hardware maintenance contracts and document and track County assets

3.0 COMPUTER INFORMATION TECHNOLOGY SECURITY POLICY

3.1 Introduction

Computer information security is the responsibility of each County Employee and contractors/vendors working with Canyon County information. Computer information security is the protection of information assets. Information assets are protected from accidental, intentional, and unauthorized disclosure, and modification or destruction including temporary loss of availability of information assets.

Information assets are computer hardware, software and data owned, leased, managed, or used by Canyon 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 are examples of Canyon County's information assets.

3.2 Objectives

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

3.3 Guidelines

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

- A. Ownership And Individual Responsibility - The accountability principle requires that there be a single point of responsibility for an asset. Therefore, Canyon 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 Canyon 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" criterion.

- Federal laws, State statutes, or County Policy which designate a Office 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 the 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 Canyon County. If more than a single County Office is involved in the creation or collection, the Office most at risk in a case of loss of the asset is the owner in the absence of any higher level of responsibility within Canyon County. In this case Offices must come to written agreement regarding information asset ownership;
- An information asset may be utilized by a person or group which is not directly a County Office. 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 Canyon County.

The Owner is charged with the following responsibilities on behalf of Canyon 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, Canyon County IT, and/or by the Canyon 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 Canyon 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 Chief Technology Officer (CTO) and/or Deputy Chief Technology Officer (DCTO). The Security Officer position/responsibility is exclusive to IT personnel.

- B. Classification of Information - Information assets may be compromised intentionally or accidentally. Each information asset has a risk associated with it in terms of the cost to Canyon 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 the 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 Canyon 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).

Exceptions to rules and procedures have probably caused the failure of more safeguards than any other problem. Canyon 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 Canyon County) must be approved by the Owner and communicated to and approved by the Board of County Commissioners who then accepts 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.
- Must meet all State (ILETS) and Federal (NCIC and FBI) Guidelines.

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 Canyon County if exposed;
- Is practically impossible to reproduce or repurchase and is still viable to the County;
- Would halt work of two or more County employees if compromised; or
- Valued at more than \$1000.
- Must meet all State (ILETS) and Federal (NCIC and FBI) Guidelines.

C. Physical Access - Access to the main computer room is restricted to authorized personnel.

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 computers from theft as well.

D. Data Access - To insure maximum information security, Canyon County administers computer security under the program of "least possible privilege to perform their job." 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 locked at night or when left unattended. 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, 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 County systems.

All data residing on County systems is the property of Canyon County and its representatives and is to be used by and for Canyon County for county purposes only.

Likewise, all email communication initiated and/or received by the County systems is the property of Canyon County and its representatives and is to be used by and for Canyon County purposes only.

E. Personal and Account 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 includes the employee's supervisor and IT personnel), or written down and placed in a visible location on or around the computer or desk.

- All passwords must be changed every 90 days;
- Passwords must be at least 8 characters in length;
- A password must be at least 2 days old before it can be changed;
- A user can not use the same password for 10 changes. This was put into place to prevent the use of the same two passwords over and over;
- Password must contain 3 of the following 5 elements:
 - English uppercase characters (A-Z)
 - English lowercase characters (a-z)
 - Base 10 digits (0 – 9)
 - Non-alphanumeric (for example: !, \$, #, or %)
 - A password may include a space, but a space does not count as any of the above elements.
- The password may not contain three or more consecutive characters from the user's account name;

- F. Data Storage - IT does not backup local hard drives. Canyon County workstations are configured to store data files on assigned network drives. These assigned network drives are backed-up each night. If a local hard drive malfunctions, the data is lost and cannot be recovered by IT.
- G. Attachment To The Canyon 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 County network must have a contract signed by The Board of Canyon 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 this IT policy statement. The County will have the right to ensure conformity with this policy. Canyon County reserves the right to deny any application for direct connection to the County network.

Canyon 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.

- H. Data Disposal - Disposal of 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. If they are being disposed of they must be damaged such that their contents are rendered unreadable. The largest opportunity for information leakage occurs in the disposal of printed reports. Particularly because Canyon 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 the County is subject to rules governing County records retention. Before disposal, please contact the Canyon County Prosecuting Attorney’s Office, Civil Division.)

- I. Computer Virus Detection - County employees will report all instances of computer virus to IT immediately. Anti-virus software must be installed on all Canyon County computers that have the potential to be connected to the network in order to detect, identify, isolate, and eradicate viruses unless there is written permission by IT. This software must be updated 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 be subject to immediate correctional measures. This includes virus checking all media and all computers which may have shared portable media with the infected computer.

- J. Personnel - Department manager or elected official, is responsible for notifying the IT Security Officer via the helpdesk 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.

4.0 E-MAIL AND ELECTRONIC DATA POLICY

4.1 Purpose

The purpose of this policy is to explain the proper use of e-mail and electronic data. Use of email on County computers is to provide business-related communications. Canyon County policies that apply to paperwork also apply to electronic data and e-mail (ref. Data Disposal section.)

Canyon County computers 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.

4.2 Appropriate Usage

Appropriate usage of e-mail is for 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.

4.3 Monitoring

E-mail may be monitored, upon request of or with the permission of an employee's elected official 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.

4.4 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 protecting the data. 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.

5.0 INTERNET POLICY

5.1 Introduction

Internet access on County computers is a privilege extended to some of the County's employees. Proper usage of the Internet is the responsibility of each Canyon 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 from the authorization of the elected official or department head.

5.2 Privacy

Employees have no right to privacy with regard to their use of the Internet on County computers. Internet usage may be monitored.

5.3 Appropriate Usage

Appropriate usage of the internet is for business-related activities. Prohibited sites include those containing offensive graphics, images, and language. Streaming or downloading of files without proper authorization is strictly prohibited.

Internet usage may be monitored, upon request of or with the permission of an employee's elected official, in order to prevent inappropriate and/or unprofessional activities over the County's Internet.

6.0 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 disciplinary proceedings, including termination of employment.

7.0 DEVIATION POLICY

There shall be absolutely no deviation from this policy without the written authorization from the BOCC or relevant elected official. Any deviation without said written authorization shall be considered non-compliance.

8.0 EMPLOYEE SIGNATURE STATEMENT

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

Change History

(Specific Changes in **Bold**)

Change	Requested By	Changed By	Date	Approved By
Initial Acceptance	BOCC	IT Dept	12/01/2009	12/01/2009