MORGAN COUNTY GOVERNMENT
Computer Policy

Morgan County Government's ("MCG") computer systems, electronic mail ("e-mail"), and internet service should only be used for County business.

On any and all MCG equipment and property, MCG has total and complete ownership rights, viewing access, and all other rights to any and all computer hardware, computer software, computer files, and documents of any nature, including but not limited to all historical internet activity as well as any and all e-mails, opened or not. No employee can have any expectation of privacy while using MCG equipment when transmitting, receiving, or storing information.

All electronic communications systems and information transmitted by, received from, and stored in these systems is owned or under the custody of MCG. MCG may monitor the system at any time at its discretion. Electronic messages or other information stored or sent by MCG computers may be public records under Colorado law, available to the public for inspection on request.

Protecting County information and systems is every employee's responsibility. Unauthorized acts against MCG, including but not limited to misuse, misappropriation, destruction of information or systems resources, and the unauthorized use of software or shareware by any employee is prohibited.

1. ACCEPTABLE USE POLICY

Users are provided access to MCG's computer network to perform job functions. Additionally, certain employees may also be provided with access to the internet and e-mail.

All computer access is for the purpose of increasing productivity and not for non-business activities. Any connection to the internet offers an opportunity for unauthorized users to view or access MCG information. Therefore, it is important that all connections be secure, controlled, and monitored.

To this end, MCG employees should have no expectation of privacy while using MCG-owned or MCG-leased equipment. Information passing through or stored on MCG equipment can and will be monitored. MCG maintains the right to monitor and review internet use and e-mail communications sent or received by employees as necessary.

1.1 Responsibilities

Morgan County Government Employees are responsible for:

- Honoring acceptable use policies of networks accessed through MCG's internet and e-mail services.
- Not overloading networks with excessive data or wasting MCG's other technical resources.
- Abiding by existing federal, state, and local telecommunications and networking laws and regulations.
- Following copyright laws regarding protected commercial software or intellectual property.
- Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of MCG's network resources. This includes, but is not limited to, instant messaging, internet radio, internet based games, internet chat rooms, and internet blogs.

2. SOFTWARE / HARDWARE POLICY

2.1 Software

All software acquired for or on behalf of MCG or developed by MCG employees or contract personnel on behalf of MCG is and shall be deemed company property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements. All software will be installed by MCG's IT staff only.

2.1.1 Purchasing

All purchasing of MCG software shall be centralized with the Information Systems department to ensure that all applications conform to corporate software standards and are purchased at the best possible price. All requests for

corporate software must be submitted by the Elected Official or Department Head to the Information Systems Director, who will then determine the standard software that best accommodates the desired request, submit budget requests for these purchases, and submit requests to the Board of County Commissioners and County Purchasing Department following the guidelines of the County Procurement Policy.

Any software residing on MCG equipment that has not been approved or authorized by the Information Systems staff will be removed without notice to the employee.

2.1.2 Licensing

No software may be copied. Any duplication of copyrighted software may be a violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of MCG's Software/Hardware Policy.

2.1.3 Software standards

The following list shows the standard suite of software installed on company computers (excluding test computers) that is fully supported by the Information Services department:

- Microsoft Windows Operating Systems
- Microsoft Office (Access, Excel, PowerPoint, Word)

Employees needing software other than those programs listed above must submit their request to their Elected Official or Department Head who will forward the request to the Information Systems Department. Each request will be considered on a case-by-case basis in conjunction with the software-purchasing section of this policy.

As of January 1, 2004, the Morgan County Information Systems Department will not be purchasing upgrades and/or licenses for applications providing the same functionality as those included in the software standards list (i.e., WordPerfect, Lotus 1-2-3, Professional File, etc.). It is the employee's responsibility to migrate to the applications included in the software standards list and the Information Systems staff will be glad to help with any file conversions. Unique situations may be evaluated on an individual basis but approval for applications providing word processing, spreadsheet, and/or database management outside of the software standards list will only be granted under extenuating circumstances.

2.2 Hardware

All hardware devices acquired for or on behalf of Morgan County Government or developed by MCG employees or contract personnel on behalf of MCG is and shall be deemed company property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

2.2.1 Purchasing

All purchasing of MCG computer hardware devices shall be centralized with the Information Systems department to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price. All requests for corporate computing hardware devices must be submitted by the Elected Official or Department Head to the Information Systems Director who will then determine standard hardware that best accommodates the desired request, submit budget requests for these purchases, and submit requests to the Board of County Commissioners and County Purchasing Department following the guidelines of the County Procurement Policy.

2.2.2 Installation and Maintenance

All computer hardware will be installed, configured and maintained by MCG IT staff only. Any computer equipment needing to be moved will be moved by MCG IT staff. This is necessary to prevent damage to equipment, cables, cards and hard drives.

2.3 Outside Equipment/Software/Electronic Files

No outside equipment may be plugged into MCG's network without the Information Services department's permission. This applies to all MCG facilities.

No outside software or files may be installed or used on MCG equipment. This includes but is not limited to any software applications, screen savers, personal picture files, etc. CD drives on all MCG computers are to be used for

data or training purposes only. It is not permissible to use CD drives to play music or entertainment videos.

2.4 Violations and Penalties

Any labor plus materials required to service MCG's computer system equipment or software resulting from inappropriate use by the end user, will be billed to the individual department.

Penalties for violating the Software/Hardware Policy will vary depending on the nature and severity of the specific violation. Any employee who violates the Software/Hardware Policy will be subject to:

(i) At the discretion of MCG's IT department, the user's access may be terminated.
(ii) Disciplinary action as described in the company's employee handbook, including but not limited to reprimand, suspension, and/or termination of employment.
(iii) Civil or criminal prosecution under federal and/or state law.

3. BACKUP POLICY

3.1 Procedure

MCG's Information Systems Department coordinates and monitors backups on all County network servers. The IS Department configures local user pc's to connect to County servers and uses logon scripts to establish drive mappings to the servers for user data storage. Therefore, all user data must be stored on County servers in order to be backed up. It is NOT the policy of the IS Department to perform backups on local user hard drives for machines that are or can be connected to a County server. The Information Systems Department performs certain periodic backups throughout the year that are stored off-site as part of the department's disaster recovery scheme.

Because the Office of Emergency Management and Building Maintenance Departments do not currently have connectivity to a County server, local backups will be performed on these machines on a monthly basis. It is the responsibility of personnel in both of these departments to contact the IS Department to schedule monthly backups. If backups are required more frequently for either department, they need to submit a request to the IS Department.

4. INTERNET AND E-MAIL

MCG employees have an obligation to use their access to the Internet and e-mail in a responsible and informed way, conforming to network etiquette, customs and courtesies, and representing the County in a positive and professional manner. Use of the internet or e-mail by a County employee constitutes acknowledgment of this policy.

4.1 Use

4.1.1 Permitted use

The internet connection and e-mail system of Morgan County Government is solely for business use.

E-mail messages reflect MCG's image. They should be composed in a professional manner. You should exercise good judgment and common sense when creating and distributing messages. E-mail is the property of MCG and should be used exclusively for work-related purposes.

Employees are strictly prohibited from sending e-mail messages of a harassing, intimidating, offensive or discriminatory nature. Such conduct, or any other conduct in violation of this policy, may result in immediate dismissal or other disciplinary measures.

It is not the policy of the Morgan County Information Systems Department to individually monitor all employee e-mail messages, but every e-mail sent and received by MCG employees will be archived on the County e-mail server and is subject to review. The Morgan County Information Systems Department maintains a list of all passwords and retains the right to access employees' e-mail without notice to the employee. Employees should NOT expect that e-mail is confidential or private.

Correspondence of employees in the form of e-mail may be a public record subject to public inspection under the Colorado Open Records Act. Correspondence of elected officials to discuss public business among them may be

subject to the open meetings law. However, e-mail communications that express an opinion or are deliberative in nature and are communicated for the purpose of assisting elected officials in reaching a decision are a work product and not a public record.

4.1.2 Prohibited use

County employee e-mails are the only e-mail accounts to be used to conduct County business. No personal e-mail accounts can be used to send or receive information pertaining to County business and personal e-mail accounts are not to be accessed using County equipment.

Employees shall NOT use MCG's Internet or e-mail services to view, download, save, receive, or send material related to or including:

- Shareware or Freeware
- Offensive content of any kind, including pornographic material.
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
- Threatening or violent behavior.
- Illegal activities.
- Commercial messages.
- Messages of a religious, political, or racial nature.
- Gambling.
- Sports, entertainment, and job information and/or sites.
- Personal financial gain.
- Forwarding e-mail chain letters.
- Spamming e-mail accounts from MCG's e-mail services or other MCG machines.
- Material protected under copyright laws.
- Sending business-sensitive information by e-mail or over the Internet.
- Dispersing confidential, secure, or private data to MCG's customers or clients without authorization.
- Opening files received from the Internet without performing a virus scan.
- Tampering with your MCG-issued account name or identification (handle) in order to misrepresent yourself and MCG to others.

4.2 E-mail Attachments

4.2.1 Permitted Use

Employees may send and receive e-mail attachments that do not exceed 10 MB in size. In the event that a user needs to receive or send an attachment larger than 10 MB, he/she will need to submit a request to the Information Systems Department for approval.

4.2.2 Protocol for Opening

E-mail attachments must be scrutinized in order to avoid virus infections where possible. The following protocol must be used when opening e-mail attachments:

- Do not open attachments from any individual with whom you are not familiar. Attachments received from an unexpected or unknown sender are not to be opened and need to be forwarded to the Information Systems Department immediately for virus checking.
- Do not open any attachment that ends in the following suffixes: .scr, .exe, .com, .pif
- If you are unsure about the validity of the attachment, seek assistance from the Information Systems Department before opening the attachment.

5. VIRUS PROTECTION POLICY

It is the responsibility of all who use MCG's computer network to take reasonable measures to protect that network from virus infections. When an infected file is opened from a computer connected to MCG's network, the virus can spread throughout the network and may do damage.

5.1 How Viruses Can Infect Morgan County Government's Network

Viruses can enter Morgan County Government's network in a variety of ways:

- **E-mail—**By far, most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect MCG's network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.
- **Disk, CD, Zip disk, or other media—**Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- **Files accessed during internet use—**Accessing files via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.

5.2 How to Respond to and Report a Virus

The Information Systems staff will attempt to notify all users of credible virus threats. Because this notification will go to everyone, employees should not forward virus warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.

As stated, it is the responsibility of all MCG network users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

- Do not open unexpected e-mail attachments, even from coworkers.
- Never open an e-mail attachment from an unknown or suspicious source.
- Never download freeware or shareware from the Internet.
- If a file you receive contains macros that you are unsure about, disable the macros.

In the event that a file containing a virus is opened that infects a local hard drive, the IS staff will perform utilities and if necessary, rebuild the machine to its original state. Because backups are not performed on users' local hard drives, any user data stored incorrectly on the local machine will be lost.

5.3 Notify the MCG Information Systems Department of all Suspicious Files

If you receive a suspicious file or e-mail attachment, DO NOT OPEN IT. Call MCG's Information Systems department and inform them that you have received a suspicious file. The Information Systems department will take the proper steps to handle the file.

If the file is an infected spreadsheet or document that is of critical importance to MCG, the Information Systems department will attempt to scan and clean the file. The Information Systems department, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on MCG computers.

6. PASSWORD POLICY

6.1 Purpose

This policy outlines the handling, responsibilities, and scope of passwords for the Information Systems Department of MCG.

6.2 Authority

This policy has full support from MCG, the Board of County Commissioners, and the Human Resources department. The Director of Information Systems administers the policy, which is currently effective for all MCG employees and computer systems.

6.3 Mission

The Information Systems Department objective is to enable MCG employees to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs and keeping information secure within our Information Systems resources. Passwords are the entry point to our Information Systems resources. Protecting access to our resources is pivotal in ensuring that our systems remain secure. While we have not been exploited, nor do we expect to be, we must be diligent in guarding access to our resources and protecting them from threats both inside and outside MCG.

6.4 Password handling

Passwords for *all* systems are subject to the following rules:

- No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. Supervisors may request passwords for users within their Department only.
- No passwords are to be shared in order to "cover" for someone out of the office. Contact Information Systems, and they will logon to the computer with an appropriate account if there are resources you need to access that are not available under your current network account.
- Password policies for user access on all MCG's systems will be established and maintained by the Information Systems Department including but not limited to user logons, file and print sharing and software access.
- Initial logon passwords will be assigned by the Information Systems Department. On any MCG systems that require the user to periodically change their password, the user must report the new password each time it is changed to the Information Systems staff so that they can perform any necessary troubleshooting procedures for such users. Failure to report such passwords will result in delays in support situations.
- Passwords are not to be displayed or concealed on your workspace.

6.5 Systems involved

MCG password policy addresses passwords for the following Information Services systems:

- **Network and client operating system**: Windows Operating System username and password.
- **Network file and print sharing**: Group and user-level security on folders, individual files and printers.
- **Outlook/Exchange groupware**: Windows username and password.

6.6 Administrative passwords

Administrative passwords are subject to stringent composition, frequent change, and limited access. This includes passwords for routers, switches, WAN links, firewalls, servers, Internet connections, administrative-level network operating system accounts, and any other Information Systems resource. All administrative passwords will be documented and stored in a secure location.

6.7 Responsibilities

The Information Systems Department has the responsibility to enforce this policy. This can be done through systematic means and interaction with MCG employees.

MCG employees are responsible for complying with this policy.

6.8 Continuance

This policy is a living document and may be modified at any time by the Morgan County Director of Information Systems, the Morgan County Board of County Commissioners, or the Human Resources department. This policy is designed to secure Morgan County Government resources. This enables MCG to achieve its business objectives. Full cooperation with this policy is appreciated so that all goals can be met in accordance with all MCG objectives.

Acknowledgment of Policy

This form is used to acknowledge receipt of and compliance with Morgan County Government's Information Systems department's Policies and Procedures, as stated above.

Procedure

Complete the following steps:

1. Read the Morgan County Government Computer Policy.
2. Sign and date this form in the spaces provided below.
3. Return this page only to the Human Resources department.

Signature

By signing below, I agree to the following terms:

- I have received and read a copy of the Morgan County Government Computer Policy and understand and agree to the same.
- I understand and agree that any software and hardware devices provided to me by Morgan County Government remain the property of Morgan County Government.
- I understand and agree that I am not to purchase, install, modify, alter, or upgrade any software programs or hardware devices provided to me by Morgan County Government.
- I understand and agree that I shall not copy, duplicate (except for backup purposes if required as part of my job) or allow anyone else to copy or duplicate any software.
- I understand and agree that if I leave Morgan County Government for any reason, I shall immediately return to Morgan County Government the original and copies of any and all software, computer materials, or computer equipment that I may have received from Morgan County Government that is either in my possession or otherwise directly or indirectly under my control.
- I understand and agree that any software programs and/or data files that I have developed and/or used during my employment with Morgan County Government are property of Morgan County Government.
- I understand and agree I must make reasonable efforts to protect all Morgan County Government-provided software and hardware devices from theft and physical damage.

_____

Employee Signature

_____

Employee Name (Printed)

_____

Employee Title

_____

Date

_____

Department