

CERRO GORDO COUNTY INFORMATION TECHNOLOGY POLICIES



IT IS THE POLICY OF THE M.I.S. DEPARTMENT UNDER THE DIRECTION OF THE BOARD OF SUPERVISORS TO PROVIDE AUTOMATED ACCESS TO ALL INFORMATION REQUIRED FOR FULLFILLING THE REQUISITES OF EACH COUNTY DEPARTMENT.

GENERAL INFORMATION TECHNOLOGY POLICY

I. Objective

The county has the obligation to ensure that its computer resources are used properly and within the guidelines established by the county. In pursuit of that goal, the county reserves the right to monitor the system for signs of illegal or unauthorized activity, which may include periodic review of the computer system and the policies that govern its use.

The county recognizes that information is an asset, and shall establish security measures and assign responsibilities to protect it from loss, theft, and unauthorized modification, misuse, or disclosure. All security measures will conform to county policies and applicable federal and state laws.

II. Scope

The Information Systems Policy applies to users and all county owned equipment, programs, and information. For the purpose of this policy 'User' shall be defined as a full-time, part-time, temporary or contract employee, whether elected or not, that have been granted access rights to the computer network and computer equipment.

The Information Services Director will maintain and update the policy and distribute it to the Personnel Department for Board of Supervisors approval and inclusion in the Cerro Gordo County policy manual.

Responsibilities

M.I.S. software responsibility:

It is the responsibility of the M.I.S. Department to provide the software, limited training, and assure functionality of all utility software. This includes the operating system, network systems, word processing software, spreadsheet, database, backups, and other software with common usage across departments. Any software systems that have been developed or modified by Cerro Gordo County M.I.S. will also be maintained and supported.

There will be no software installed on the network or individual hard drives (whether or not the PC is attached to the network) without full knowledge of the MIS Dept.. All software must be approved by the M.I.S. Department and virus checked prior to installation.

It will be the responsibility of M.I.S. to register and track all licenses required for the county network. If unlicensed or illegal software is found on county equipment, the department head will be notified, and if it is not or cannot be corrected, it will be removed.

All software installations will be requested by the elected official/department head (or their designee) of the department where it will be used.

M.I.S. hardware responsibility:

The hardware responsibility of the M.I.S. Department includes support of all county owned and approved computer equipment used by the county whether or not it is attached to the network. The network includes local hard and floppy disk drives in individual PC's. To fulfill this responsibility, the following rules will be applied:

All computer related equipment must be purchased through the M.I.S. Department.

All hardware connected to the network must be installed and attached by the M.I.S. Department with written authorization by the elected official/department head (or their designee) of the department where it will be used.

All defaults set by MIS must be left as set when installed.

If specific hardware is required for a function relating to the county system, the elected official/department head (or their designee) will provide written authorization to M.I.S. of the requirement and all appropriate steps will be taken to acquire, install, and prepare for maintenance of the required equipment.

User responsibility:

All users are responsible for safeguarding information and the physical assets that store this information. Users are responsible for using computing resources in an effective and lawful manner, consistent with the provisions of this policy.

All users understand that there is no right of privacy associated with the county's computer equipment, the Internet, electronic mail, or any other communications devices. In this regard, the county has the right to monitor all communications, retain records of all communications, and use this information in any manner permitted by law.

Compliance

Users shall comply with all sections of this policy. Violations of this policy may result in disciplinary action up to and including termination. Violations may result in termination of system access and/or criminal prosecution as deemed appropriate by the county.

III. Security

A. Physical Security

Department Heads and Elected Officials shall be responsible for all hardware assigned to their department. The MIS Department will secure all hardware not assigned to a particular department. All data including disks, tapes, data, etc. will be stored in a secured and/or locked environment. Data may not be removed from county premises without permission of the department head.

B. Network Security

The MIS Department shall assess risks to information from network, remote, and Internet connections and shall implement effective measures to protect the county's information. All users shall be granted their own user account on the Cerro Gordo County network upon receipt, in the MIS Department, of a written request from the Department Manager (or approved designee), and after the acknowledgement sheet for this policy has been signed by the user and filed with the MIS Department. Users must select a secure password and shall not divulge that password to anyone, except upon order of their department supervisor. The password must be changed on 90-day intervals. All computers should be "logged out or otherwise secured" if the user is away from their normal work area for a period exceeding 15 minutes.

C. Software Security

Commercial Software will be used in accordance with licensing agreements and copyright law. Noncommercial and personal commercial software will not be installed on computers unless previously approved in writing by the MIS Department. Users shall not download software from the Internet without the permission of the MIS Department.

D. MIS Steering Committee

Cerro Gordo County has established and maintains a MIS Steering committee to oversee security procedures, review supplemental department policy, and provide a forum for establishing general direction and priorities.

E. Security Awareness

Department Heads and Elected Officials shall ensure that all users in their departments are aware of and comply with security measures. HIPAA training must be taken within a reasonable period after being accepted for a position within the county. The period shall not exceed 90 days.

F. Laptop Computer Security

MIS will setup and maintain a BIOS password on all laptop computers purchased for county use. In addition, a USB flash drive will be purchased with each laptop. The flash drive will be used for storage of county information (there should be no county information stored on the laptop's hard drive). When the laptop is not in use, the flash drive must be disconnected and kept in a separate location. The flash drive can then be used in a standard work station and the data uploaded (moved) to the user's network files. All reasonable effort will be made to secure the laptop from theft. Some of these efforts may include locking the laptop in your trunk when you must leave it in your car, use a locking cable to affix the laptop to a stationary object, carry the laptop in a regular case that does not appear to be a laptop case.

Disaster Backup

The MIS Department shall maintain backups of all critical data on a scheduled basis

Personal Use of Computers

Information, equipment, software and any other Information Technology resources may be used for business purposes only. It is understood that the County's computers, computer network, and other computer resources may not be used for personal purposes without the explicit permission of the Department Head and knowledge of the MIS Department. (IA Code Sec. 721.2(5))

No personal files will be left on either the internal hard drive or any networked disk drive.

The system may not be used for any political purposes. (IA Code Section 721.2(8))

No software may be loaded or run on the system without first being approved by M.I.S.

IV. Prohibited

It is not possible to list all behaviors that are prohibited or considered unacceptable. This list is representative of the types of activities which may result in corrective action and is not intended to be all-inclusive.

- A. Use of a computer account or the county's network in a manner which violates federal, state or local law or county policy,
- B. Transfer or use of copy written materials through the county's computer resources, without the explicit consent of the owner,
- C. Harassment of another user via computer and/or network facilities,
- D. Taking or altering another's work without permission,
- E. Attempting to gain another user's password or log on as another user,
- F. Permitting use of an assigned account by another person,
- G. Use of an account for commercial purposes,
- H. Physical abuse of the county's computer equipment.
- I. Use of County computers for any illegal activity. If evidence of such activity is found, all legal remedies will be taken.

V. Regulations on the use of Information Systems

All electronic communications and data maintained by county personnel are protected by security systems requiring passwords. A different password is required to be assigned to each individual who accesses the computer system. Any misuse or disclosure of a person's password is a breach of the security of the computer system, and subjects the employee to possible disciplinary action, up to and including termination. Additionally, any attempt to defeat the password system is an act of misconduct.

All disks that are inserted into the county's computers must first be scanned for viruses.

Users shall not obstruct or disrupt the use of any county system or network.

Users shall not attempt to alter without proper authorization from MIS, either the hardware or software components of the county's computing system or network.

The MIS Department reserves the right to inspect any and all files stored in private areas of the network to assure compliance with the policy.

The MIS Department must approve all users requiring external network use, prior to execution.

VI. Electronic Mail (E-Mail)

Cerro Gordo County provides e-mail for all employees for the purpose of conducting county business. The E-mail system includes messages that are generated within the network as well as those that originate, or are sent to the Internet. Employees are to use e-mail as they would any other type of official county communications tool. This means that when any e-mail is transmitted, both the reader and sender should consider and assume that any e-mail could be made available to the public (including a court of law). Usage of e-mail to distribute system wide messages will be reviewed in advance by the respective department head.

INTERNET/E-MAIL POLICY

Purpose

The county provides electronic mail to employees at county expense for their use in performing their duties for the county. E-mail used in the Cerro Gordo County system integrates the use of Internet e-mail along with internal e-mail. The purpose of this policy is to provide general information regarding the use and limitations.

Background

In connection with your work at Cerro Gordo County you may also have full Browser access to the Internet through the use of county computers. This allows for some very positive and effective aspects while at the same time allowing options that can be used in a very negative manner.

Loosely defined, the Internet is a web of connected computers throughout the world. Literally millions of computer users have access to virtually any information regarding any subject. The Internet can provide access to libraries in New York, Tokyo, and Brazil, as well as provide access to forms from the Internal Revenue service, regulations from the Department of Transportation, and items too numerous to mention. While the Internet can serve as a useful tool in connection with your employment, it can also serve as a serious distraction.

Responsibilities

Much of the information available on the Internet is free of charge to the user. There are, however, a number of services that require payment for information obtained. While certain services may claim that providing financial information is "secure", there is no guarantee that any confidential information such as bank account numbers, credit card numbers, or other personally secured items can be protected from unauthorized use once they are transmitted on the Internet. Employees may not transmit any confidential county information over the Internet. This includes, but is not limited to, bank account numbers, credit card numbers, financial information, or any other confidential information regarding any department or employee of Cerro Gordo County

The Internet can also provide access to material, which may be deemed offensive to others. You are cautioned that information that may be sexually explicit or otherwise offensive can be obtained. It is strictly against the county's policy for employees to attempt to access, copy, or distribute such offensive material.

There are numerous gambling sights on the internet. Visiting these sites is not a valid use of county time and under certain circumstances, may be illegal. Use of these sites is against the policy of Cerro Gordo County.

There is also information on the Internet, which may be protected by trademark or copyright laws. Illegal or unauthorized duplication of material thus protected is specifically prohibited by law and by the policies of Cerro Gordo County.

Downloading of information and programs from the Internet should be done with caution. Computer viruses can be transmitted through the downloading of programs, and the viruses may have a devastating effect on the county's computers and networks. If you must download information from the net, you must take all necessary precautions to avoid downloading a virus. Contact the Network Administrator for the best procedure to avoid duplication of a computer virus.

Supervisors or Department Heads may authorize the use of e-mail to send and receive messages and to subscribe to listserves from recognized professional organizations and entities relating to the official duties of the county. All employees are authorized to use e-mail as they would any other official county communication tool. Communication by e-mail is encouraged when it results in the most efficient or effective means of communication. The sender of e-mail messages must retain the primary responsibility for ensuring that the intended-receiver receives communication.

Employees should be aware that others might read e-mail messages for a variety of valid reasons. Although this statement is true of many other types of county correspondence also, the nature of e-mail can lead one to forget or ignore that e-mail cannot be considered the private property of the sender or recipient, even though passwords or encryption codes are used for security reasons. E-mail may be reviewed without the permission of the user. However, any internal disclosure without the consent of the sender will be limited to those employees who have a need to access the information. In most cases, information transmitted via e-mail through the county system is considered public record under state law.

Should employees make incidental use of e-mail to transmit personal messages, such messages will be treated no differently than other messages, and may be accessed, reviewed, copied, deleted, or disclosed. You should not expect that a message would not be disclosed or read by others beyond its original intended recipients.

Any use of the Internet to obtain or send offensive or sexually explicit material is expressly prohibited.

Use of the internet for any illegal activity is strictly forbidden, and if found, all legal remedies will be taken.

E-Mail can be used during discovery in a court of law, and the county will disclose any mail message to law enforcement officials if legally required. When under legal obligation, the Director of MIS will review requests for access to the contents of electronic mail without the consent of a sender/recipient.

Heavy usage or high volume activities must be kept to a minimum in order to maintain reasonable Internet response time across the network. Examples of such activities include, but are not limited to, listening to the radio over the internet, live video, downloading extremely large files, etc.

Prohibited use of e-mail

It is not possible to list all behaviors that are prohibited or considered unacceptable. This list is representative of the types of activities which may result in corrective action and is not intended to be all-inclusive

1. Use of e-mail to send chain letters.
2. Use of e-mail to send copies of documents in violation of copyright laws.
3. Use of e-mail that would compromise the integrity of the county and its business in any way.
4. Use of the e-mail system for "moonlighting", job searches, or the advertisement of personal business. (IA Code Sec. 721.2(5))
5. Use of the e-mail system to send messages containing offensive, abusive, threatening, harassing or other language inappropriate for the county.
6. Intercepting, eavesdropping, recording, altering another person's e-mail message.
7. Forwarding a message sent to you without the sender's permission.
8. Adopting the identity of another person on any e-mail message, attempting to send electronic mail anonymously, or using another person's password.
9. Misrepresenting your affiliation on any e-mail message.
10. Using e-mail for any commercial promotional purpose, including personal messages offering to buy or sell goods or services.

This policy does not constitute a contract, and the county reserves the right to change the policy at any time. Violations of this policy will be reviewed on a case-by-case basis and can result in disciplinary action up to and including termination. All e-mail messages are subject to all state and federal laws and rules, which may apply to the use of e-mail. In addition, violations of this policy or misuse of the e-mail system, which are of a criminal nature, may be referred for criminal prosecution.

CERRO GORDO COUNTY INFORMATION TECHNOLOGY, INTERNET/E-MAIL POLICY

I hereby acknowledge that I have received a copy of the Cerro Gordo County Information Technology and Internet/E-Mail policy. I understand that the county has the right to monitor the system for illegal or unauthorized activity, including periodic review of the computer system. I understand that all internet, e-mail communication systems and all information transmitted by, received from, or stored in these systems are the property of Cerro Gordo County. I have no expectation of privacy in connection with the use of this equipment or with the transmission, receipt or storage of information in this equipment. I agree to not use a code, access a file or retrieve any stored communication unless authorized. I acknowledge and consent to the county monitoring my use of e-mail at any time as provided by the e-mail policy. Such monitoring may include printing and reading all electronic mail entering, leaving or stored on the county's system. I understand that this policy shall not be construed to be a contract and may be modified by the Cerro Gordo County Board of Supervisors at any time.

I have read and understand all the provisions specified in this policy.

Employee Job Title
Employee Signature

Date

I hereby authorize access to the following:

(Printed Employee Name)

First

Last

System Login Yes No
 Internet Yes No
 Alias Yes No
 CMS Yes No
 Finance Yes No
 CATS Yes No
 GIS Yes No
 VIMS Yes No
 CIVIL Yes No

Docket Yes No
 Vanguard Yes No
 ProVal Plus Yes No
 Paperclip Yes No
 Farms Yes No
 COMIS Yes No
 I-Voter Yes No
 Other
 Other

Supervisor/Head of Department

Date