WELD COUNTY
CODE ORDINANCE 2018-06

IN THE MATTER OF REPEALING AND REENACTING, WITH AMENDMENTS, CHAPTER 9 INFORMATION TECHNOLOGY, OF THE WELD COUNTY CODE

BE IT ORDAINED BY THE BOARD OF COUNTY COMMISSIONERS OF THE COUNTY OF WELD, STATE OF COLORADO:

WHEREAS, the Board of County Commissioners of the County of Weld, State of Colorado, pursuant to Colorado statute and the Weld County Home Rule Charter, is vested with the authority of administering the affairs of Weld County, Colorado, and

WHEREAS, the Board of County Commissioners, on December 28, 2000, adopted Weld County Code Ordinance 2000-1, enacting a comprehensive Code for the County of Weld, including the codification of all previously adopted ordinances of a general and permanent nature enacted on or before said date of adoption, and

WHEREAS, the Weld County Code is in need of revision and clarification with regard to procedures, terms, and requirements therein.

NOW, THEREFORE, BE IT ORDAINED by the Board of County Commissioners of the County of Weld, State of Colorado, that certain existing Chapters of the Weld County Code be, and hereby are, repealed and re-enacted, with amendments, and the various Chapters are revised to read as follows.

CHAPTER 9
INFORMATION TECHNOLOGY

Repeal and Replace Article I – Information Technology, in its entirety, as follows:

Article I

Weld County Information Technology Acceptable Use Policy

Sec. 9-1-10. General Provisions.

A. The Information Technology Acceptable Use Policy is to be followed by ALL employees (full time, part time, seasonal, temporary, interns), elected officials, contractors, vendors, and other authorized individuals ("Users") who utilize any information technology (IT), electronic, or other communication device owned and provided by Weld County, or who are granted access to any Local Area Networks and/or Wide Area Networks or other technology services maintained and provided by Weld County.

B. This policy applies to any activity performed from a County-owned computing device or personally owned computing device that is connected to, or has access to, the County computing network. Additional policies related to information technology must be approved

4427941 Pages: 1 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

cc: CTB(EG/CH), FI(DW), ACT(BC), CA(All), IT(RR) 9/10/18

by Information Technology and the Board of County Commissioners, based on internal business needs.

Responding to security incidents. All security incidents shall be reported to the Information Technology Technical Support Center for immediate review and response. Information Technology employees will follow the Computer Incident Response Plan to address any IT security related events. ANY USER FOUND VIOLATING THIS POLICY MAY FACE SANCTIONS WHICH SHALL INCLUDE, BUT ARE NOT LIMITED TO, DISCIPLINARY ACTION BASED ON PROVISIONS OF HUMAN RESOURCE RULES, DEVICE REVOCATION OR SERVICE ACCESS TERMINATION, AND/OR LEGAL ACTION.

Sec. 9-1-20. Ownership of Devices and Services.

A. All IT and communication devices and services, including, but not limited to, computers, peripherals, cell phones, pagers, software, files, e-mail messages, internet activity logs, remote access, and any other data or records stored on devices or other media provided by Weld County regardless of their physical location, or the form in which they are maintained, are considered property of Weld County and are owned exclusively by Weld County.

B. USERS HAVE NO EXPECTATION OF PRIVACY WHEN USING ANY INFORMATION TECHNOLOGY OR COMMUNICATION DEVICE, SERVICE, SYSTEM, NETWORK, FILE, OR ANY OTHER DATA OWNED BY WELD COUNTY. The County, as directed by the Board of County Commissioners, reserves the right to access, review, delete, and/or disclose any files, records, e-mail messages, or other data without notice to, or authorization from, a User, and to seize any IT or communication devices provided by Weld County. This right continues after the User ceases to have access to a device or service provided by Weld County.

Sec. 9-1-30. Organizations Affected.

A. The scope of this policy defines the obligations of Users, as defined in Section 9-1-10, in using County Information Technology resources owned, managed, supported, maintained or operated by Weld County Information Technology. While this policy contains specific information regarding expected use of Weld IT resources, Users must follow and stay current on all additional requirements stated in Weld County Cyber-Security guidelines and standard operating procedures which are available on the County Intranet.

Sec. 9-1-40. Authorized County Network Access.

A. Authorized access to the County network for new Users must be approved by the department head, elected official, or designated person in the department. Requests for new employee security, or changes to existing security, must be submitted using the online IT Security Request Form.

   1. All documentation authorizing User access to controlled computing and information resources must be archived and retrievable upon request for all accounts. Requests will be retained for a period of seven (7) years.

   2. Login passwords must meet the County required standard as set forth in Section 9-1-50.

4427941 Pages: 2 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

3. Generic and shared accounts are strictly prohibited. All User IDs must uniquely identify Users to the system, unless specified by the Chief Information Officer and/or the IT Security Manager.

B. All IT security requests for user terminations within the County's operations must be submitted to the Department of Human Resources who will then coordinate with Information Technology. Upon the termination of an employee, the employee's access to all accounts, including remote access and e-mail, will be immediately suspended. All devices must be gathered and returned to IT immediately. The department head or elected official must coordinate with Human Resources, IT, and Legal Counsel prior to destruction or reassignment of any hardware, device, or electronic information.

Sec. 9-1-50. Guidelines

A. Responding to security incidents. All security incidents shall be reported to the Information Technology Technical Support Center for immediate review and response. Information Technology employees will follow the Computer Incident Response Plan to address any IT security related events.

B. Responding to violations. All Users must play an active role in helping to assure the security and quality of all County applications by reporting any violations of this policy. In doing so, Users help to assure the optimum performance and availability of County systems.

C. User obligation to report security and policy violations. Any User who observes violations of the IT Acceptable Use Policy should report the violation to his or her supervisor or Information Technology.

D. User responsibility. The security, protection, and integrity of County information assets are the responsibility of all Users. It is each User's responsibility to fully understand the information security policies contained in this Article and to apply these policies effectively to his or her daily practices and routines.

E. Manager responsibility. It is the responsibility of all managers to ensure all Users under their supervision fully understand and follow these information security policies. Managers are responsible for keeping their Users informed on any changes regarding these policies. Should any User consistently not adhere to County policy, the manager shall take appropriate remedial steps. It is the responsibility of all managers to ensure all information assets under their purview are secured and managed to ensure compliance with relevant policies and procedures.

F. Use of information systems and resources. Any User who is allowed to use County computing systems to perform the necessary functions identified with his or her position must not misuse or abuse computing systems and resources.

G. Compliance with software copyrights and licenses. All Users must comply with, and respect, the copyright laws and license agreements of the software licensed to the County for use on business computing systems.

4427941 Pages: 3 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

1. Use of illegal software. Users must not download and/or install pirated or illegal software or software that violates existing copyright or license agreements.

2. Use of nonapproved software. The County strictly forbids the downloading or installation of non-County-owned, non-County-licensed, or other unapproved software on County computing systems without prior consent from Information Technology. Applications which are no cost and do not threaten security of the computing system may be installed unless IT objects.

H. Acceptable use of passwords. Each password owner is required to safeguard and protect each password he or she has created or that is entrusted to him or her. Password sharing and account sharing is strictly prohibited. Writing down passwords is not an acceptable practice.

I. Security of the computer through locking practices and mechanisms. All Users of a computing system must either lock the computing device, or logoff the system, when away from a computer device for any length of time.

J. HIPAA systems. Computing systems covered by HIPAA must employ the use of a locking screensaver or similar mechanism to automatically enable after a minimum usage lapse of five (5) minutes. All other County systems will be fifteen (15) minutes, unless specified by Information Technology.

K. Transmission of sensitive information over unsecured networks. Users must not send sensitive information over unsecured networks without the use of encryption technologies to secure the transmission. Such examples would be, but are not limited to:

1. Sending credit card information over the Internet.

2. Sending confidential business information over unsecured, non-County networks.

3. Sending information via e-mail without applying the appropriate security protocols.

Any questions about whether information should be encrypted or secured should be referred to Information Technology.

L. Tampering with security mechanisms. All County computing systems are equipped with security mechanisms to protect the information and resources of each system. Users shall not tamper with, reconfigure or disable such mechanisms. Such mechanisms would include, but not be limited to, anti-virus software, encryption and access controls.

M. Prohibited Activity. The following are prohibited:

1. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail phishing, etc.).

2. Circumventing User authentication or security of any host, network or account.

3. Introducing honeypots, honeynets, or similar technology on the network is prohibited.

4427941 Pages: 4 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

4. Providing access to another individual, either deliberately, or through failure, to secure access.

5. Accessing a server or an administrative account for any purpose other than conducting County business, even with authorized access.

N. Illegal access of computer systems. County computing systems must not be used to obtain illegal access to computer systems, to interfere with the normal operations of computer systems, or to perform malicious acts against a computer system.

O. Unauthorized testing of computing system security. Users shall never test the security of computer systems, whether physical or logic based, without written permission from the Information Technology Security Manager and the senior management of both the facility from where the test is being launched, and the facility where the system resides.

P. Disclosure of Attorney-Client privilege information. Users must never disclose information that could be considered classified or proprietary to unauthorized persons.

Q. Disclosure of classified information. Users must never disclose information that could be considered sensitive, classified, or proprietary to unauthorized persons.

R. Use of system. Data is intended to be accessed, used, and shared only to the extent that it is authorized and necessary to fulfill a User's assigned job duties.

S. System changes. Any software that allows configuration changes to networks, computers and other hardware or software, should only be installed by members of Information Technology.

T. Workstation reallocation. Information Technology is responsible for maintaining all computing hardware on the County network. A User may not remove or retain hardware or software without County IT permission. The procedure for the reallocation of a workstation is as follows:

1. Remove PC from location.

2. Re-format hard drive and re-image for new User.

3. Redeploy to new location.

U. Security breaches and disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular assigned duties. Disruption includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

V. Use of e-mail systems and resources. Users with legitimate business needs for a County e-mail account may have the use of the County e-mail system. Such usage is for enhancing productivity and communication. Users shall not misuse or abuse e-mail systems and resources.

4427941 Pages: 5 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

1. *Electronic mail (e-mail)* is defined as any message that is transmitted electronically between two (2) or more computers or terminals, whether stored digitally or converted to hard (paper) copy.

2. Under Part 2, Article 72, Title 24, C.R.S., e-mail messages may be considered public record and may be subject to public inspection. Users must be aware of the potential public release of their emails. All computer-related information, including e-mail messages and/or digitally stored documents, are the property of the County and are considered the County's records, even if the information resides on privately owned devices. County e-mail should remain within the County e-mail system until archived or deleted.

3. E-mail messages that concern policies, decision-making, specific case files, contracts or other information that should be kept as part of the official records of County business, shall be retained within the County's e-mail archiving system by the recipients of such e-mail.

4. E-mail messages will be automatically deleted by the e-mail system on the 90th day following receipt, unless stored within the County's e-mail archiving system.

5. The Board of County Commissioners retain ultimate authority over all electronically and digitally stored e-mails, except for emails containing criminal justice information.

6. For purposes of open records requests, either the department head or designated data/records steward is the custodian. Information Technology will assist in retrieving any data and information.

7. Users must cooperate in the preservation and retention of any hardware, information, or documentation related to potential litigation. This includes maintaining any hardware, e-mail, electronic files or other information.

8. As with any County property or equipment, e-mail is intended to be used for official County business only. Strictly forbidden e-mail usage includes transmission of political messages, solicitation of funds for political or other purposes, or sending of harassing messages.

    a. Users must refrain from sending e-mail messages that are considered lewd, offensive or harassing.

    b. Users must not participate in sending, forwarding or responding to e-mails that are of a disruptive or coercive nature; such as, the distribution of spam or chain letters.

    c. The County identifies passwords as highly sensitive information. Account owners shall never divulge their e-mail account passwords and login information.

9. Users must never share e-mail accounts.

10. E-mail is County property. The County has the right to inspect and review any e-mail or other data stored on County computers and equipment or on privately owned devices if used for County business. Additionally, County officials may inspect and copy e-mail and computer records when there are indications of impropriety by a User, when substantive

4427941 Pages: 6 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

information must be located and no other means are readily available, or when necessary for conducting County business. Supervisors may review the contents of an employee's electronic mail, without the employee's consent, with the approval of the Department Head, the Director of Human Resources and/or County Legal Counsel.

W. Use of Internet systems and resources. Users shall not misuse or abuse County Internet resources, which could result in disciplinary action by the County.

1. Acceptable Internet connectivity. Users access to the Internet is intended for County business, through authorized County gateways.

2. Personal use of Internet connectivity. Use of County computing resources to access the Internet is intended for legitimate County business purposes only.

3. Affiliation with the County. Users may make public their affiliation with the County in work-related mailing lists and other work-related communication resources on the Internet.

4. Inappropriate use of Internet resources. Users initiating or participating in communications of an inappropriate nature, or in an unprofessional way are strictly prohibited. Users must refrain from the use of lewd, offensive or hostile language when communicating using County resources. Likewise, all Internet messages that are intended to harass, annoy or alarm persons are prohibited.

5. Inappropriate use of Internet resources for illegal access. Users are strictly prohibited from contacting or probing information systems with the intent to gain unauthorized access. Users must not attempt to disrupt, or interfere with, the operation or function of any information systems.

X. Use of networked systems and network related resources. Users must not misuse or abuse networked systems and network related resources. This could result in disciplinary action by the County, pursuant to Chapter 3 of the Weld County Code.

1. Disregard for security mechanisms. Users must not attempt to bypass security mechanisms.

2. Use of encryption for highly sensitive information. It is the responsibility of all Users to take the necessary precautions to encrypt highly sensitive information.

3. Network privacy. All communications using County resources may be monitored for statistical, legal and investigative purposes. Users should expect no right of privacy to communications made using County equipment and resources. The County retains the right to preserve, catalogue, and distribute any County-owned information or resource.

Y. Use of remote access (VPN). Remote access into County networks is only permissible through an Information Technology-administered VPN (Virtual Private Network) solution.

Z. Compliance with software licenses. Each department is responsible to ensure that all software licenses are complied with.

4427941 Pages: 7 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

Sec. 9-1-50. Password Policy.

A. All passwords must conform to the requirements described below. This includes County-owned systems that are managed outside of IT, as well as IT-managed systems. Any User found to have violated this policy may be subject to disciplinary action, pursuant to Chapter 3 of the Weld County Code.

1. Password Creation Requirements.

a. Must be a minimum of nine (9) characters in length.

b. Must possess a minimum of three (3) of these four (4) characteristics:

1) One lower case letter.

2) One upper case letter.

3) One number.

4) One special character.

2. Password must be changed every 90 days.

Sec. 9-1-60. County network and Internet security.

A. Access to inappropriate and malicious websites for Users is prohibited.

B. The Board of County Commissioners is the only authority that can approve changes to the default filter restrictions applied to Users Internet access.

C. All remote access must follow the guidelines of the Acceptable Use Policy.

D. Users shall not access malicious websites, files or other potentially malicious content. Such activity is a direct violation of this policy and may result in disciplinary action.

Sec. 9-1-70. Physical and Environmental Security Policy.

A. Internal security operations. All County facilities must be secured, as appropriate, to prevent unauthorized access to County information computing systems, resources and networks, including the wireless network.

1. All information technology equipment must be purchased by Information Technology. (See Section 9-9-10.)

a. Only County devices with approved wireless adaptors are allowed on the wireless network.

b. Approved devices will be configured by Information Technology for secure access to the County wireless network.

4427941 Pages: 8 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

c. Guest wireless access is permissible in certain areas of the County wireless network. Guest wireless is restricted to web browsing only and is provided on a limited basis.

d. All policies and procedures for accessing the County network apply for wireless access.

B. Computing in public and untrusted zones. The County operates several computing systems. There are computing systems in public access areas. There are also computing systems within the County jail for inmate use.

C. Public computing systems. The County operates several public access computers which are available for use by the public, within County facilities. These systems, due to the uncontrolled nature of their use, must be segregated to an isolated or physically separate segment of the County network. All access to internal County resources must be tightly controlled and limited, to prevent any misuse of these systems. Auditing must be enabled on these systems.

D. Inmate computing systems. The County provides several computers for the use of inmates within the County jail. Due to the uncontrolled use of these systems, all inmate computing systems must only maintain a minimal set of computer resources to prevent abuse of such systems and resources. This would include:

1. Computers must not maintain any unnecessary ports or peripherals, including a CD-ROM drive, floppy drive, serial ports, USB ports, modems or other nonessential interfaces.

2. Computers must not have access to other computing systems or servers, except to accomplish the specific purpose for the inmate computing systems.

3. Computers must not have Internet access.

4. Network access must be segregated from the other County network segments.

E. Security zones. Specified areas within a facility that are designated as performing critical functions, or that contain sensitive information or systems, must make use of security mechanisms and procedures. These zones must be isolated by security controls of reduced permission from the general facility population. Permission must be based on the need to physically access the area for a job function. Such security zones would include server rooms and the communications closets. Access to these areas is controlled by the Department of Buildings and Grounds, in conjunction with Information Technology. Information Technology monitors all access. Access is limited to the following Information Technology employees via proximity card security:

1. Chief Information Officer.

2. Information Technology Security Manager.

3. Technical Director.

4. System Administrators.

4427941 Pages: 9 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

5. Network Specialist.

6. Vendors working with Information Technology who require access to server rooms will be escorted by one (1) of the above authorized employees, and will be required to sign and date the access log located outside of the secured area.

F. Equipment security. All information-computing equipment, and any information contained or processed by the equipment, must be reasonably protected from damage, interruption and interception.

G. Secure disposal of computing equipment. All County computing equipment, including phones, and peripherals, must be disposed of securely by IT personnel to prevent unauthorized access to any residual company information.

1. Hard drives. Prior to the disposal of any hard drive or disk drive, the device must either be physically destroyed or formatted to current Department of Defense standards. This is to be performed only by Information Technology.

2. Optical media. Prior to the disposal of any optical media, such as CD-ROMs or DVDs, these devices must be physically destroyed. This may be accomplished using shredding or incineration.

3. RAM. Prior to disposal, all Random-Access Memory modules must be destroyed. This includes all memory devices; such as, memory from computers, memory from printers and FAX machines, or other memory devices. This is to be performed only by Information Technology.

4. Secure disposal of computing equipment. All County computing equipment, including phones and peripherals, must be disposed of securely by IT personnel to prevent unauthorized access to any residual company information.

H. Data security and protection guidelines.

1. Information Technology is responsible for ensuring that all County data on the network is backed up.

2. Backup retention is as follows:

a. Incremental daily backups: one (1) week on site.

b. Weekly full backups: one (1) month on site.

c. Monthly full backups: one (1) year.

d. Annual full backups: seven (7) years.

3. Backup storage will be as follows:

a. Weekly and monthly backups will be retained on site up to three (3) months.

4427941 Pages: 10 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

b. All other monthly and annual backups will be stored off site.

4. For any major changes to a server or application, a full backup is run prior to changes being completed.

Section 9-1-80. Definitions.

A. LAN - A Local Area Network (LAN) is a computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings.

A LAN is composed of inter-connected workstations and personal computers which are each capable of accessing and sharing data and devices; such as, printers, scanners and data storage devices, anywhere on the LAN. LANs are characterized by higher communication and data transfer rates and the lack of any need for leased communication lines.

B. WAN - A Wide Area Network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LANs). This ensures that computers and Users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.

C. Encryption - the process of converting information or data into a code, especially to prevent unauthorized access.

D. Computing Device - a unit of hardware, outside or inside the case or housing for the essential computer (processor, memory, and data paths) that can provide input to the essential computer, or of receiving output, or of both.

E. Computing Network - a set of computers connected for sharing resources. The most common resource shared is connection to LAN and WAN. Other shared resources can include a printer, a file server, or database server.

F. Honeypot – a computer security mechanism set to detect, deflect, or in some manner, counteract attempts at unauthorized use of computing networks. Generally, a honeypot consists of data which appears to be a legitimate part of the site, but is isolated and monitored, and that seems to contain information, or a resource of value to attackers, who are then blocked.

G. Phishing - the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information; such as, passwords and credit card numbers.

H. Security Incident - An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction

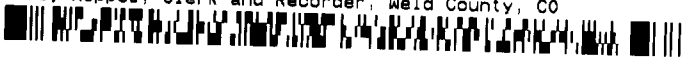
4427941 Pages: 11 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO

of information, interference with information technology operations, or significant violation of responsible use policy.

BE IT FURTHER ORDAINED by the Board that the Clerk to the Board be, and hereby is, directed to arrange for Municode to supplement the Weld County Code with the amendments contained herein, to coincide with chapters, articles, divisions, sections, and subsections as they currently exist within said Code; and to resolve any inconsistencies regarding capitalization, grammar, and numbering or placement of chapters, articles, divisions, sections, and subsections in said Code.

BE IT FURTHER ORDAINED by the Board, if any section, subsection, paragraph, sentence, clause, or phrase of this Ordinance is for any reason held or decided to be unconstitutional, such decision shall not affect the validity of the remaining portions hereof. The Board of County Commissioners hereby declares that it would have enacted this Ordinance in each and every section, subsection, paragraph, sentence, clause, and phrase thereof irrespective of the fact that any one or more sections, subsections, paragraphs, sentences, clauses, or phrases might be declared to be unconstitutional or invalid.

4427941 Pages: 12 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO



The above and foregoing Ordinance Number 2018-06 was, on motion duly made and seconded, adopted by the following vote on the 13th day of August, A.D., 2018.

BOARD OF COUNTY COMMISSIONERS
WELD COUNTY, COLORADO

ATTEST: Esther E. Gesick

Weld County Clerk to the Board

BY: Lee A. Rempel
Deputy Clerk to the Board

APPROVED AS TO FORM

Asst. County Attorney

Date of signature: 08/20/18

Steve Moreno, Chair

Barbara Kirkmeyer, Pro-Tem

Sean P. Conway

Julie A. Cozad

Mike Freeman

First Reading:	July 2, 2018
Publication:	July 11, 2018, in the Greeley Tribune
Second Reading:	July 23, 2018
Publication:	August 1, 2018, in the Greeley Tribune
Final Reading:	August 13, 2018
Publication:	August 22, 2018, in the Greeley Tribune
Effective:	August 27, 2018

4427941 Pages: 13 of 13
09/04/2018 11:32 AM R Fee:$0.00
Carly Koppes, Clerk and Recorder, Weld County, CO