



# Information Technology

## Acceptable Use Policies and Procedures

The following *Information Technology Acceptable Use Policies and Procedures* are to be followed by ALL employees, contractors, vendors, and other authorized individuals (“Users”) who utilize any information technology (IT), electronic, or other communication device owned and provided by the City and County of Denver, or who are granted access to any Local Area Network and/or Wide Area Network (“LAN/WAN”) or other service maintained and provided by the City and County of Denver. It is expected that all City and County of Denver agencies and departments will enforce these policies at a minimum. However, the various City and County of Denver agencies and departments may enhance and strengthen these policies and procedures, based on internal business needs. These policies are to be used in conjunction with Career Service Authority Rule 15-80 (Code of Conduct: Electronic Communications Policy) and Executive Order 16.

*ANY USER FOUND VIOLATING THESE POLICIES OR PROCEDURES WILL FACE SANCTION WHICH MAY INCLUDE DISCIPLINARY ACTION BASED ON PROVISIONS OF CAREER SERVICE RULES, DEVICE REVOCATION OR SERVICE ACCESS TERMINATION, AND/OR LEGAL ACTION.*

### **Ownership of Devices and Services**

All IT and communication devices and services, including (but not limited to) computers, peripherals, PDA devices, 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 the City and County of Denver regardless of their physical location or the form in which they are maintained, are considered property of the City and County of Denver and are owned exclusively by the City and County of Denver.

USERS SHOULD HAVE NO EXPECTATION OF PRIVACY WHEN USING ANY IT OR COMMUNICATION DEVICE, SERVICE, SYSTEM, NETWORK, FILE, OR ANY OTHER DATA (INCLUDING E-MAIL MESSAGES) OWNED BY THE CITY AND COUNTY OF DENVER. The City and County of Denver 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 the City and County of Denver. This right continues after the User ceases to have access to a device or service provided by the City and County of Denver.

### **Access to Devices and Services**

Use of IT or communication devices and access to the LAN/WAN and other services are restricted to those employees who have been authorized by their agency or department supervisor or to those contractors who have been authorized by their contract manager. Users will only be granted access to the resources required to perform job / contractual duties.

Supervisors or contract managers shall formally request from the appropriate Technology Services personnel all needed IT devices and access rights for new Users.

Each new User shall sign the most current version of the *Information Technology Acceptable Use Acknowledgement* prior to being given access to IT devices or services. Existing Users shall sign an updated *Acknowledgement* upon any material change being made to these *Policies and Procedures*. Signed *Acknowledgements* will be maintained by Technology Services, copies will be provided to the User, and to the employee's Human Resources Department or contractor's contract manager upon request. Users may also have to sign additional Acknowledgements / Agreements required by specific City and County of Denver Agencies and Departments.

The User and the User's supervisor or contract manager share responsibility for immediately notifying the appropriate Technology Services personnel of any changes in the User's status, including: name change, transfer to another position, termination of employment or contract, or any changes in the User's responsibilities which would alter the access rights required.

For transferring employees, the User's previous supervisor shall immediately notify the appropriate Technology Services personnel of all IT and communication devices, services, and access rights the User has, the name and title of the User's new supervisor, and the date of the transfer. The User's new supervisor must request from the appropriate Technology Services personnel all needed IT and communication devices, services, and access rights now required for the User.

For employees who will no longer be working for the City and County of Denver, the User's supervisor shall immediately notify the appropriate Technology Services personnel of all IT and communication devices, services, and access rights the User has and the date the User's access is to be terminated. Upon the termination date, Technology Services will deactivate the User's account. It is the User's responsibility to return any PDA devices, cell phones, pagers, or other portable devices provided by the City and County of Denver to the User's supervisor or appropriate Technology Services personnel. After the User's account has been deactivated, Technology Services will download all email messages and files contained on the User's assigned network drive and desktop computer hard drive onto a CD to be handed over to the User's supervisor or contract manager. The User's assigned network drive and desktop computer hard drive will then be overwritten or deleted permanently. It is the supervisor's responsibility to transfer any needed files to another network drive within 30 days, at which time the CD should be destroyed.

The City and County of Denver will take reasonable steps necessary to accommodate all Users and ensure compliance with the Americans with Disabilities Act. These accommodations will be provided on a case-by-case basis.

### **Use of Devices and Services**

Users shall not make unauthorized use of or knowingly permit unauthorized use of IT or communication devices, services, software, files, or any other data or records stored on equipment provided by the City and County of Denver including that on disposable or portable storage media. Except as indicated below, Users may only access, use, disclose, and/or delete files, records, or other data that is created, received, maintained, or transmitted on behalf of the City and County of Denver as required to perform authorized responsibilities.

Users shall not use any IT or communication device, service, software, file, or other data or records owned by the City and County of Denver in order to gain personal or financial benefit for the User or anyone else.

IT and communication devices and services (including use of e-mail and the Internet) are provided to Users to aid in the performance of City business. Limited, occasional or incidental use for personal, non-business purposes is allowed so long as it is of a reasonable duration and frequency, does not interfere with the performance of job duties, does not violate any laws or regulations, and is not in support of a personal business. Personal, non-City business use of IT and communication devices, services, software, e-mail, and the Internet shall be limited to use before scheduled work hours, during breaks, lunch, and after scheduled work hours.

Users shall use their assigned e-mail account in an appropriate manner. Users shall not knowingly transmit, retrieve, or store any communication that is: discriminatory or harassing; derogatory to any individual or group; obscene or pornographic; vulgar or profane; defamatory or threatening; in violation of another User's privacy; used in order to propagate any virus, worm, Trojan horse, or trap-door program code; used to plagiarize or copy copyright-protected material; or used for personal profit or illegal purposes. Users may forward or redistribute e-mail messages received by them only when doing so fulfills a legitimate business need of the City and County of Denver. No personal messages, chain letters, or other unauthorized broadcast messages may be forwarded from a User's e-mail account.

As City and County of Denver e-mail messages are not encrypted at this time, Users shall refrain from transmitting external e-mail messages that contain personally identifiable information. Social Security Numbers should NEVER be included in external e-mail messages.

When sending e-mail, Users shall take all reasonable steps to confirm the accuracy of all e-mail addresses. If a User discovers an e-mail has been sent in error, the recipient is to be contacted and requested to delete the e-mail message immediately.

Users shall ensure that all external e-mail messages contain an attached signature with the sender's name, title, phone number, users should also consider the following confidentiality statement, which individual agencies may require: "This e-mail transmission from the City and County of Denver, and any documents, files, or previous e-mail messages attached to it, are intended solely for the individual(s) to whom it is addressed and may contain information that is confidential, legally privileged, and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any unauthorized review, forwarding, printing, copying, distribution, or use of this transmission or the information it contains is strictly prohibited. A misdirected transmission does not constitute waiver of any applicable privilege. If you received this transmission in error, please immediately notify the sender and delete the original transmission and its attachments. Thank you." Signatures shall not include any photos, pictures, graphics, or other text unless approved by the Denver Marketing Office.

Accessing any inappropriate Internet site is prohibited, including sites that are obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable. Inappropriate use of the Internet also includes participation in "chat rooms" not related to assigned job responsibilities; playing games; selling, or promoting the sale of merchandise for personal gain; downloading music, games, pictures, video, freeware, or software; or using instant messaging. Users who intentionally visit inappropriate sites or use the Internet in an inappropriate manner will face sanction. (This restriction does not apply to Users who have a legitimate business need to access otherwise prohibited Internet sites and who have approval from their agency or department Executive Director and Technology Services.)

The City and County of Denver uses independently supplied software and data as a web filter to block certain inappropriate categories of Internet sites. A User who has a legitimate business need to access a blocked site may submit a written request, approved by the User's agency or department Executive Director, to the Technology Services Security Manager to have the site

unblocked. The fact that a site is not blocked does not imply that it is acceptable or permissible to access.

All User access of the Internet will be recorded in an Internet activity log which is available for review by designated Technology Services personnel upon request by a supervisor or Executive Director. When inappropriate use of the Internet is found, Technology Services will notify the User and the User's supervisor of the inappropriate use. After the third inappropriate use notification, or upon supervisor request, Technology Services shall disable all User Internet access. Access to the Internet may be restored upon written request from the User's agency or department Executive Director to the Technology Services Security Manager.

### **Electronic Records**

Definition, Electronic Records: are a subset of Records, same in all respects except that their physical form is electronic. The term includes all original email, documents, papers, letters, books, maps, photographs, sound or video recordings or other information that are created or received by the City and County of Denver in the exercise of City functions in electronic form, regardless of whether public access to them is open or restricted under the laws of the State of Colorado. The term "Electronic Record" is subject to the Public Records Act as set forth in C.R.S. as amended, Section 24-72-201 through 206.

Users shall save all Electronic Records and other necessary files to an assigned network drive or other encrypted electronic media that is designated and approved by User's department or agency. Files saved to desktop computer hard drives will not be backed up or protected and may be lost in the event of a computer failure or other event.

Users must save and delete Electronic Records and E-mail in accordance with Executive Order 64. Any electronic documents that are not considered to be Electronic Records or otherwise necessary to do business shall not be retained.

Users will be held accountable and face possible discipline for any unauthorized files saved on their assigned network drive, other shared drives, or desktop computer hard drive, including (but not limited to) pictures, audio clips, video files, and copyright-protected material owned by another party.

Users may save information on disposable or portable media (floppy disks, CDs, external drives, DVDs, zip disks, removable thumb drives, flash memory drives, USB memory drives) if necessary for a business purpose, upon supervisor approval, and only for as long as is necessary based on the retention requirements of the information type stored per Executive Order 64. Confidential information should be saved in an encrypted form or to encrypted media. Disposable media containing information that is the property of the City and County of Denver must be stored in a locked area, may only be removed from the user's office location if authorized by the User's supervisor to do so, and must be destroyed if no longer useful once the retention deadline is met.

### **Security of Devices and Services**

All City and County of Denver agency and department computer hardware, PDA or other portable device, and other peripheral device purchases must be coordinated with Technology Services to maintain system compatibility throughout the City and County of Denver network. Users shall not attempt to install or attach any unauthorized external device to a City and County of Denver computer without prior written authorization from Technology Services. All hardware upgrades and additions must be installed by Technology Services personnel. Users shall not attempt any network-related computer repairs without Technology Services

authorization. Technology Services personnel may disconnect or otherwise disable any device that poses a threat to the City and County of Denver network.

Attaching modems to City and County of Denver computers will only be done by exception and only with authorization from Technology Services. Computers may either be plugged into the LAN/WAN or a phone line but not both simultaneously.

Only software licensed to the City and County of Denver may be installed on City and County of Denver computers, PDA devices, or other peripheral devices. Users shall not attempt to install, add, or use any unauthorized software of any kind (including screen savers) on City and County of Denver computers, PDA devices, or other peripheral devices. Users shall not copy, duplicate, distribute, delete, or modify any proprietary or other software licensed to the City and County of Denver, or related documentation, without written authorization from the vendor and Technology Services.

Users shall not use any IT device that another User has already logged onto and shall not use another User's User ID and password to log onto a workstation computer for any reason. The only exception will be for appropriate Technology Services personnel providing requested technical support. In the event that a User suspects another person knows and/or has used his/her User ID and password, the User must notify his/her supervisor, the appropriate Technology Services personnel, and any other appropriate departmental personnel immediately.

Users shall practice adequate password management by keeping all passwords confidential. Users shall keep all passwords physically secure and not place a written list of passwords in plain view or anywhere easily discoverable (for example, posted under a computer keyboard). Users shall not disclose system passwords to anyone, for any reason. Users must contact their supervisor, appropriate Technology Services personnel, and any other appropriate departmental personnel immediately if anyone asks for, or attempts to "verify" a User's password.

Users should not choose passwords that can be easily guessed by a third party or that are related to the User's job or personal life. For example, a car license plate, a spouse's name, or a home address should not be used. Passwords should not follow a consistent pattern (January2006, February2006, March2006, etc.) Under no circumstances should a Social Security Number be used as a password.

Users shall construct passwords with at least eight (8) characters, including three of the following four character types: upper case alphabetic, lower case alphabetic, numeric, special characters (symbols, punctuation marks). For additional security, Users are recommended to create "pass phrases" that contain at least fifteen (15) characters. Passwords are case sensitive. Passwords will expire after 90 days and Users will not be permitted to reuse any of the last fifteen (15) passwords used. After five (5) failed login attempts, the User's account will be disabled. The User must then personally contact Technology Services to manually reset their account.

Users shall not disclose their voice mail passwords unless it is a shared phone line, unless a supervisor requests access to a voice mailbox in support of specific business operations, or unless someone is covering a phone for the User for a specific, temporary length of time. In the latter case, the voice mail password must be changed immediately upon the period ending.

Users shall not leave any IT device logged into the network and unattended for an extended period of time. When leaving a work area, Users must log out or invoke a password-protected screen saver on any IT devices in that area that are under the User's control. All City and County of Denver workstation computers will automatically launch a screensaver after fifteen

(15) minutes of nonuse. Users are encouraged to “force” their computers into a screensaver (Ctrl +Tab) if they know they are leaving the computer unattended for any period of time.

Users shall log off workstation computers at the conclusion of each work day.

City and County of Denver servers and network equipment shall be located in limited-access areas that are only accessible to certain authorized Technology Services personnel. All City and County of Denver servers will be backed-up daily and all information stored on servers will be retained for fourteen (14) days, or such other period as may be determined by Technology Services, before permanent deletion. All scheduled archival back-up media will be stored securely in an off-site location.

The City and County of Denver Technology Services Division shall automatically check and implement system security patches as necessary. Servers will be protected by a comprehensive firewall. Servers will be scanned on a regular basis and maintain up to date anti-virus software that will constantly monitor for active viruses. Updates will be unobtrusively deployed.

An activity log will be created by the City and County of Denver system that contains sufficient information for after-the-fact investigation of unauthorized activity or loss. The system will securely log all significant computer security-related events. Log entries will provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with these policies and procedures. Examples of computer security-related events may include: successful and unsuccessful session log-ins; identification and authentication failures; security administration activity; all activities performed by privileged users; and failed attempts to access information. Information captured for each logged event may include: User ID, network address, information or system accessed, date and time of access, type of event, result of event, and reason for failure. Authentication information, such as passwords, must never appear as part of an activity log. For critical or sensitive applications or resources, logs should be generated for all access, additions, modifications, and deletions whether authorized or unauthorized. Logs will be reviewed periodically for anomalies, or as part of a security incident response.

Before a workstation computer is transferred to a new user, surplus, or disposed of, all data files on the hard drive will be overwritten or destroyed by the appropriate Technology Services personnel. Operable hard drives must be overwritten prior to being provided to a new user. If the hard drive is to be removed from City service entirely, it must be overwritten to Department of Defense standards or physically destroyed.

The City and County of Denver Technology Services Division has the right to update the system and/or network at any time.

### **Remote Access**

*All Information Technology Acceptable Use Policies and Procedures* within this document apply equally to desktop IT and communication devices and services as well as to laptops, peripheral devices, and other portable devices used outside of a City and County of Denver office or building.

Users requesting laptop computers, cell phones, or other portable devices must have written approval from an agency or department Executive Director and must coordinate the purchase of remote devices with Technology Services to maintain system compatibility throughout the City and County of Denver network. Laptop computers, cell phones, or other portable devices provided to staff for use out of a City and County of Denver office site are to be used primarily for City business.

Users shall not save any public records, personally identifiable information, or other files to a laptop or peripheral hard drive for any longer than absolutely necessary. All such information must be saved to the User's assigned City and County of Denver network drive as soon as possible. Laptops and portable media such as USB drives or portable hard disks pose a security risk in that they are easily stolen or lost. As a result, extra precautions must be taken with such devices and should not be left unattended or in a non-secured environment.

Users shall provide appropriate security at their remote sites, including updated anti-virus software, must not have a "split tunnel" configuration, and those installations with Cable/DSL/T-1 or other high speed connections must have a firewall. (Split Tunnel Configuration: A computer that is accessing the City and County of Denver network is itself accessible on the Internet. Many Cable/DSL connections are configured this way. Users should check with their network administrator for instructions on how to block this.)

Any vendor requesting remote access to a City and County of Denver server must utilize current virus protection, security updates and patches, and robust firewall software on the vendor's computers and/or server that will be used to access the network. If malicious code such as viruses, Trojans, worms, or backdoors are introduced by the vendor and compromise or put at risk the City and County of Denver's proprietary information, the City and County of Denver will seek any civil and criminal remedy available.

Vendors with remote access to a City and County of Denver server must keep strictly confidential any records, proprietary information, and technology provided to them, and must use such information solely for the purpose the information has been provided. The termination of the vendor's contract with the City and County of Denver does not relieve the vendor from this obligation.

The Technology Services Helpdesk will provide User assistance remotely as requested. However, it is not the responsibility or duty of Technology Services to physically assist User's in their homes in order to gain remote access to the City and County of Denver network.

Technology Services personnel may revoke a User's remote access privileges at any time and without warning if a threat to the City and County of Denver network is found or suspected.

## **Violations**

Users shall immediately report any violations, or suspected violations of these *Information Technology Acceptable Use Policies and Procedures* to a supervisor, the Technology Services Helpdesk, the Technology Services Security Administrator, and/or any other appropriate departmental personnel.

City employees who violate these *Information Technology Acceptable Use Policies and Procedures* may be subject to disciplinary action based on provisions of Career Service Rules, device revocation or service access termination, and/or legal action.

Devices, services, systems, networks, files, or any other data owned by the City and County of Denver must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other jurisdiction in any material way. Use of any resources owned by the City and County of Denver for illegal activity is grounds for immediate dismissal. The City and County of Denver will cooperate fully with any legitimate law enforcement inquiry in this regard.

## **Other**

Technology Services shall publish the most current version of this document on an annual basis and provide to all Users. The City and County of Denver reserves the right to revise and modify this document at any time.



## Information Technology Acceptable Use Acknowledgment

By signing this *Acknowledgement*, the User named below consents and agrees to be bound by all current *Information Technology Acceptable Use Policies and Procedures*. The User understands that any failure to adhere to the *Policies and Procedures* may result in disciplinary action based on provisions of Career Service Rules, device revocation or service access termination, and/or legal action.

This *Acknowledgement* applies to any IT and communication devices and services the User is provided by the City and County of Denver, including (but not limited to) computers, peripherals, PDA devices, cell phones, and pagers; software; files; e-mail messages; Internet activity logs; remote access; and any other data or records stored on or created with devices provided by the City and County of Denver.

The User shall sign this *Acknowledgement* and be provided a copy of the most current *Policies and Procedures* prior to being given access to any IT or communication device or service by the City and County of Denver, and shall sign an updated *Acknowledgement* upon any material change being made to the *Policies and Procedures*. Refusal to sign this *Acknowledgement* will result in no IT or communication device or service being provided by the City and County of Denver. Refusal to sign this *Acknowledgement* or updated *Acknowledgement* may result in disciplinary action based on provisions of Career Service Rules, device revocation or service access termination, and/or legal action.

DATE: \_\_\_\_\_

USER LEGAL NAME: \_\_\_\_\_

USER SIGNATURE: \_\_\_\_\_

DEPT / AGENCY: \_\_\_\_\_

EMPLOYEE ID NUMBER (if known): \_\_\_\_\_

TERMINATION OF ACCESS DATE (if applicable): \_\_\_\_\_

Original: Technology Services

Copy: User

Copy: Human Resources (upon request)