



Administrative Regulation
City Managers Office
Division of Information Systems
1015 Eleventh Ave
Delano, CA 93215
www.CityofDelano.org

INFORMATION TECHNOLOGY POLICY

1.0 Purpose

This policy governs the operation and/or use of the City of Delano's information technology, including but not limited to computer hardware and software systems, networks, internal and external e-mail, Internet/Intranet/Extranet-related systems as well as communications-related tools and other electronic media such as Personal Digital Assistants (PDAs), desk phones, cell phones, pagers, facsimile, copiers and voice mail collectively referred to as Information Technology Systems. These systems are to be used for business purposes in serving the interests of the City in the course of normal operations.

The purpose of this policy is to outline acceptable use of information technology at the City of Delano. These rules are in place to protect both the employee and City of Delano. Inappropriate use of information technology exposes the City of Delano to risks including computer viruses, compromise of network systems and services, and legal issues. This policy also serves as a means to notify employees that they have no right to privacy in the use of the information technology systems. This policy also advises employees that the City reserves the right, with or without notice, to access, monitor, review, copy and/or delete any computer files, including e-mail, all website communications and/or transactions on information technology systems. In addition, employees are advised that there may be circumstances under which the information stored on the City's Information Technology Systems may be required to be publicly disclosed under the Public Records Act or litigation.

2.0 Scope

This policy applies to employees, council members, contractors, consultants, temporaries, and other workers at the City of Delano, including all personnel affiliated with third parties who use or operate a City Information Technology Systems ("Users"). This policy applies to all equipment that is owned or leased by the City of Delano.

3.0 Policy

3.1 General Use and Ownership

1. It shall be the policy of the City of Delano that the use of all City Information Technology Systems shall be for City-related purposes.
2. Information Technology Systems are the sole property of the City. The City reserves all rights, including termination of service without notice, on all Information Technology Systems that it owns and operates. This policy shall not be construed as a waiver of any rights of the City, nor shall it conflict with applicable law.

3. For security and network maintenance purposes, individuals authorized by the City Manager may monitor any Information Technology System with or without notice to the user.
4. The City reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
5. The City may suspend without notice Information Technology Systems privileges of a user for reasons relating to suspected violation of City policies, contractual agreements, local, state, or federal laws. Restriction of a specified source does not imply approval of other non-restricted sources.
6. Any attempt to access a website that has been filtered by the network website filtering software, or any attempt to bypass the City network filtering measures by the use of software or hardware designed for the purpose of bypassing City filtering measures is prohibited. Should the need arise to access a filtered/prohibited website, the User should contact his or her supervisor and gain official authorization from the City Manager or Department Director to have the Information Systems Division allow the necessary access for the prescribed period of time. Users are prohibited from intentionally accessing any internet sites that are discriminatory or offensive in nature, or promote or advocate any form or type of discrimination, sexual harassment, or disparaging.

3.2 Security and Confidential Information

1. The user interface for information contained on Information Technology Systems should be classified as either confidential or non-confidential, as defined by City confidentiality guidelines, details of which can be found in the City's Human Resource's policies.
2. User's shall keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed on a consistent basis (at least every six months).
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature should be set at 30 minutes or less, the user should log off/lock when computers are unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised in making sure such information and equipment remains secure.
5. Users should not use a City of Delano email address to post to news groups, chat rooms or web logs unless they have received proper authorization from their Department Director and is within the scope of their duties.
6. All hosts used by Users that are connected to the City network, whether owned by the User or City of Delano, shall be scanned on a regular basis by an approved virus-scanning software with a current virus definition.
7. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
8. Lost or stolen Information Technology Systems must be reported immediately to Information Systems staff and/or the City Manager. All information on such devices needs to be disclosed to the City so it can be determined if any breach of security has been made. This will allow Information Systems staff to make any necessary changes in protocol to ensure no further damage to the City's network will occur.

3.3. Unacceptable Use of E-mail, Internet, or Communication Systems

The following activities, in general, are prohibited. Users may be exempted by the City Manager from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a User authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City of Delano-owned resources.

The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use of internet technology systems.

- a. To access any obscene or pornographic material;
- b. To transmit sexually explicit images, message or cartoons, ethnic or racial slurs, or anything that may be construed as harassment or disparaging of others based on their race, national origin, ethnic group identification, religion, age, sex, sexual orientation, marital status, color or physical or mental disability;
- c. To conduct personal business;
- d. To play games;
- e. To conduct illegal activities (such as, but not limited to, gambling) or commit a crime or fraud, or violate any federal, state, or local law.
- f. Unless authorized by the City Manager, to use the username or password of another User to gain access to their e-mail or any other computer account without the User's consent;
- g. To transmit sensitive or privileged information to unauthorized persons or organizations;
- h. To download or otherwise acquire software without prior consent of the Department Head and Information Systems Manager or their designees;
- i. To use the internet in any manner that causes confidential or sensitive information to be subject to eavesdropping or interception by unauthorized individuals;
- j. To access Social Networking sites such as but not limited to Face book, MySpace, and Twitter unless it is related to City business;
- k. To stream internet radio or video for personal use.

3.4 Email and Tele Communication Activities

All e-mail business communications to non-City Users should use an appropriate professional tone, correct spelling and proper grammar. E-mail is very effective for sharing information, but less effective in resolving conflicts or differences of opinion.

When transmitting messages via e-mail, Users should be aware that e-mail messages may be read by persons other than the addressee. E-mail messages including (but not limited to) information relative to public projects or policy-making decisions may be subject to disclosure under the California Public Records Act (Government Code section 6250 et seq.) E-mail messages may also be subject to disclosure in litigation or administrative proceedings in the same manner as other City records.

There should be no expectation of privacy in the use of communications, electronically or by other means. Users should not use e-mail to create or transmit information they wish to keep private. Do not put into an e-mail anything you would not put into a hard-copy memorandum or letter.

All City business that is conducted through electronic messages should be done through a City approved e-mail account. The use of personal or non-City accounts to conduct official City business is strictly prohibited. This includes the use of Hotmail, Yahoo, and/or G-Mail accounts that are not explicitly monitored by the City.

E-mail to and received from attorneys representing the City are privileged communications. Such e-mail communications shall not be distributed or copied to unauthorized individuals.

The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

- a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- c. Unauthorized use, or forging, of email header information.
- d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- f. Use of unsolicited email originating from within the City's networks.
- g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3.4.1 E-Mail Retention

E-mail generates correspondence and other documentation, which may be recognized as official City records requiring protection/retention in accordance with the California Public Records Act and the City's Record Retention Program. It is the responsibility of individual Users and their department heads to determine if e-mail is an official City record that must be retained in accordance with the City's Record Retention Program. The City Clerk and City Attorney can assist you in making such a determination. Preliminary drafts, notes or interagency or intra-agency memoranda

that are not retained by the City in the ordinary course of business are generally not considered to be official City records subject to disclosure and should be deleted.

Although the use of e-mail is considered official City business, the e-mail system is intended as a medium of communication. Therefore, the e-mail system shall not be used for the electronic storage or maintenance of documentation, including, but not limited to official City records.

If an e-mail message, including any attachments thereto, is to be considered an official City record, such e-mails shall be printed as a hard copy, filed, and retained in accordance with the City's Records Retention Program. The sender of the e-mail is responsible for printing and filing it accordingly. Recipients may, at their discretion, retain a hard copy of the e-mail.

Users are responsible for the management of their mailboxes. Users shall keep their Inbox, Sent Items, and Deleted Items folders free of aged e-mail. The automated mailbox management policy is as follows:

- All items in the Inbox, Sent Items, and Deleted Items folders in the user's mailbox will be automatically deleted after 30 days.
- Items in the Deleted Items folder are permanently deleted after 30 days.
- A warning will be sent to the user when the storage size of their mailbox approaches 500 megabytes.
- If the mailbox continues to grow beyond 500 megabytes, the user may not be able to send or receive e-mail.

Periodically, the City receives requests for inspection of production of documents pursuant to the Public Records Act, as well as demands by subpoena or court order for such documents. In the event such a request or demand is made for e-mail, the User having control over such e-mail, once they become aware of the request or demand, shall use their best efforts, by any reasonable means available, to temporarily preserve any e-mail which is in existence until it is determined whether such e-mail is subject to preservation, public inspection or disclosure. The City Clerk shall be contacted regarding any such e-mails within the User's control.

It is against City policy for any person to knowingly or corruptly alter, destroy, mutilate, or conceal a record, document or other object, or attempts to do so with the intent to impair the object's integrity or availability of the use in an official proceeding.

3.4.2 Ownership, Confidentiality and Disclosure

The Information Technology System is the property of the City and all information is subject to review, monitoring, and audit.

The City, through its managers and supervisors, reserves the right to review the contents of User e-mail communications when necessary for City business purposes.

Information Systems staff has the ability to extract these documents when requested by the City Manager during the retention period.

Supervisors shall have the authority to inspect the content of any e-mail message belonging to a subordinate. Therefore, Users should exercise discretion in their use of the system.

Information Systems staff will at all times maintain the confidentiality of e-mail messages residing on the system. Such items will not be casually examined or disclosed by any Information Systems staff, regardless of access capability.

Designated Information Systems staff may access and review content of e-mail messages while following procedures only when authorized by the City Manager.

Users who have left City employment, regardless of reason, have no right to the contents of their e-mail messages.

Upon leaving employment with the City, a user's e-mail messages may be accessed for the purpose of saving those messages that pertain to City business. These files may be subject to transfer to another User if necessary to conduct City business.

4.0 Brown Act

The California Ralph M. Brown Act requires that all City Council meetings be open and public. The Act expressly prohibits meetings among a quorum of Council members that are not open to the public whether that quorum of Council members communicates directly, through personal intermediaries or through technical devices. The California Attorney General has issued an opinion concluding that a majority of a local legislative body such as a City Council who email each other in order to develop a collective concurrence as to action to be taken by the City Council violates the Brown Act.

E-mail is a form of communication that may create a meeting subject to the provisions of the Brown Act. The following procedures are to be followed:

Council members and commissioners may use City e-mail systems and other services to distribute information, schedule meetings, and communicate on an individual basis with City staff provided that positions are not polled and decisions that require public deliberation by the full council or commissions are not made.

A maximum of less than a quorum of the council or commissions may communicate regarding any public business outside of a legally posted open public meeting; however, great care should be used to avoid the communication by a quorum of members on any such topic.

City Council members and/or commissioners may not make a collective decision, develop a collective concurrence on a matter, or take an actual vote via City e-mail systems of services.

A quorum of City Council members and/or commissioners may not make any series of communications regarding a decision, collective concurrence on a matter, consensus or vote via City e-mail systems or services. Such may constitute a serial meeting in violation of the Brown Act.

5.0 Enforcement

Any Users found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Procedure and Responsibilities

Requests for adding or removing Users to or from the City's Information Systems Network, including user accounts and e-mail systems, must be submitted in writing via an IT Authorization Form to the Information Systems Administrator. A copy of the form can be obtained from the Information Systems staff.

Users are added and removed from the City Network when requested and approved by the appropriate Department Head or Supervisor.

**CITY OF DELANO
 INFORMATION TECHNOLOGY SYSTEMS AGREEMENT
 NEW AND TERMINATING EMPLOYEES**

Employee Name	Department/Division	Start Date

- Establish Domain User Account
- Establish E-Mail Account
- Establish Internet Connection
- Establish Remote User Access (for mid-management & department heads only)

Employee Name	Department/Division	Termination Date

- Discontinue Domain User Account
- Discontinue Internal/External E-Mail Account
- Disconnect Internet Connection
- Discontinue Remote User Access (for mid-management & department heads only)

Approvals

Department Head Signature: _____ Date: _____

IT Administrator Signature: _____ Date: _____

Employee/Contractor Signature: _____ Date: _____

Acknowledgement:

I certify that I have received, read, and agree to abide by the City of Delano's Information Technology Policy as set forth above.