

Information Technology Regulations

400.1 PURPOSE

These regulations provide employees with requirements and standards for utilizing the City's computers, networks, electronic equipment devices, internet, intranet, storage devices, electronic mail services, communication devices and other information technology. This policy should be applied consistently with other City policies and regulations, including any that may govern the City's management of its information systems.

These regulations provide general guidelines and examples of acceptable and prohibited use for illustrative purposes but do not attempt to state all potential uses.

400.2 EMPLOYEE ACCESS

The level of access which employees are granted to the City of Tolleson's Computers, Networks and Information Services, Internet, E-mail, File Servers, City's information systems is based upon the specific employee job requirements and access will be determined by respective Department Director and/or Director of Information Technology.

Employee access to the City's computers, networks and information services is provided for work related communication, research and data retrieval. Any use that is consistent with the goals of the City of Tolleson in providing services and within the regulations is encouraged.

400.3 INFORMATION TECHNOLOGY USAGE

The City of Tolleson provides Information Technology resources for employees' official City business. Limited or incidental use of Internet services for personal, non-business purposes is acceptable. However, *personal use must be infrequent* and must not involve any prohibited activity, interfere with productivity of the employee or his/her co-workers, consume system resources or storage capacity on an ongoing basis, or involve large file transfers or otherwise deplete system resources available for business purposes.

The following uses are examples of those that are prohibited, and which may lead to discipline including termination of employment:

- (a) Any use that is illegal or in violation of City of Tolleson policies.
- (b) Any illegal use of information technology systems or services such as copyright violations and/or violations of software licensing.
- (c) Copying, downloading, installing/removing software or applications without permission from the Information Technology director.
- (d) Any use involving materials that are obscene, sexually explicit, sexually suggestive or that which may be racially or gender-based insensitive, or insensitive regarding any other protected employment category such as age, disability, religion, or national origin.

Information Technology Regulations

- (e) Misuse and/or sharing of computer passwords/accounts including accessing the systems and/or data of other users without permission or authorization from the Information Technology System Administrator.
- (f) Effecting security breaches or disruptions of network communication on computer systems both internal and external to the City of Tolleson. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server, network equipment, or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- (g) Port scanning or security scanning of computer systems both internal and external to the City of Tolleson is expressly prohibited unless performed by the Information Technology Department as part of its regular duties.
- (h) Executing any form of network monitoring which will intercept data not intended for the employee's host.
- (i) Any inappropriate communications with other staff, non-city personnel and minors. A communication is inappropriate if it would meet any of the misuse examples provided in this regulation or comparable unprofessional conduct.
- (j) Any use for private or commercial financial gain or commercial advertising which includes solicitation.
- (k) Any use as a forum for personal communications by e-mail, chat or other medium whether to internal or external parties to solicit, advocate or communicate the views of an individual or non-city sponsored organization whether for profit or not.
- (l) Providing e-mail addresses of city employees to outside parties whose intent is to communicate with city staff on non-city purposes. Using city e-mail addresses for personal use or registration for non-city business related accounts of any kind.
- (m) Forwarding e-mail attachments which contain executable files from unidentified and/or unsolicited sources that may contain malicious software code (i.e. viruses, spyware, adware, and similar software).
- (n) Sending of mass e-mail to users in and out of the City of Tolleson network for non-city business.
- (o) Malicious use or damage to City's computers, networks and information services.
- (p) Attempts to access inappropriate websites or encouraging others to do so.
- (q) Communications that do not adhere to professional standards.
- (r) Failing to report misuse, unauthorized activity, breach or attempt to breach computer security to the department director and the Information Technology director.
- (s) Using City computers, networks, electronic equipment devices and information services after such access has been denied or revoked.
- (t) Any attempt to delete, erase or otherwise conceal any information stored on a City computer that violates these regulations.

Information Technology Regulations

- (u) Connecting or installing personal laptops or wireless devices using the City internet services or network services without prior consent through the Information Technology Department.

The following are also some examples of content deemed inappropriate:

- (a) Visiting adult pornographic material(s), websites, or posting or viewing anything which is reasonably construed, within the context of a professional work environment, as sexually explicit, scandalous, defamatory, libelous, illegal or immoral, or includes material that is obscene, sexually explicit, sexually suggestive or that which may be racially or gender-based insensitive, or insensitive regarding any other protected employment category such as age, disability, religion, or national origin.
- (b) Any activity which would violate any federal, state, or local law.
- (c) Using the computer to view or send material that involves hate or discrimination
- (d) Threats of violence
- (e) Gambling
- (f) Playing Computer Games
- (g) Sending Humor oriented e-mails or links, including comics
- (h) Using the computer for buying or selling illegal drugs, alcohol, and tobacco
- (i) Dating/relationships websites or media
- (j) Any use of the computer to buy, secure, or sell weapons of any kind
- (k) Issuing or sending Chain mail, practical jokes and other frivolous messages

Any use that is determined not to be city business and inconsistent with the City's goals and regulations, which results in an intentional breach, any attempt to breach the system security, any damage to information systems, equipment, network and other information services is understood to be prohibited.

400.4 NO EXPECTATION OF PRIVACY

The City of Tolleson retains control, custody and supervision of all computers, networks, communication devices and information services owned or leased by the City. The City reserves the right to monitor all information technology and internet activity by employees and other systems users, without prior notice. The City also reserves the right to access information technology and data to update and maintain equipment without notice. Employees have no expectation of privacy in their use of City information technology, including e-mail messages, internet communications and stored files.

400.5 CONFIDENTIALITY OF INFORMATION

Employees are expected to use appropriate judgment and caution in communications to staff, business associates and residents of the City of Tolleson. Employees are aware that personal identifiable information remains confidential. Records and other documents stored electronically

Information Technology Regulations

that are sensitive in nature are to be treated in the same manner. Every reasonable effort will be undertaken to maintain information in a secure manner.

400.6 PUBLIC RECORD NATURE OF EMAIL/CONFIDENTIALITY

Email may be subject to disclosure pursuant to the public records laws as enacted under Title 39 of the Arizona Revised Statutes. A public record is a document that is made in the course of performing a duty, the immediate purpose of which is to disseminate information to the public or to serve as a memorial of official transactions for public record.

If an email is considered a public record, the City may be required to disclose the email upon request. If the context of the email is considered a public record, you must retain the record for the period of time as required by the retention schedule for the record.

400.7 COMPENSATION FOR LOSSES, COSTS, AND/DAMAGES

The employee may be responsible for any losses, costs or damages incurred by the city related to employee violations of the city "Employee Computer and Information Services Use Policy". This will be determined once damage assessment has been done by the Information Technology Department.

400.8 CITY ASSUMES NO RESPONSIBILITY FOR UNAUTHORIZED CHARGES, COSTS, OR ILLEGAL USE

The City of Tolleson assumes no responsibility for any unauthorized charges made by the employees including but not limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations and/or violations of software licensing.

400.9 EMPLOYEE QUESTIONS

Employees having questions regarding acceptable computer activity may seek further guidance from the Department Director and/or Information Technology Department.

400.10 DISCIPLINARY ACTION

Failure to comply with the City's Employee Computer and Information Services Use policy may result in disciplinary action, up to and including termination. Illegal use of the City's computers may also result in referral to law enforcement authorities.

400.11 EMAIL ARCHIVING AND RETENTION POLICY

All employees need to be aware of this policy so that they can take appropriate action to promptly save e-mails that need to be retained in connection with any State law, contractual requirements or any other applicable retention schedule. The obligation to retain a particular e-mail will generally be the same as the retention obligation for records in any other format that document the same program function or activity. Any and all e-mails that are the subject to a Litigation Hold will not be subject to the terms of this policy from the effective date of the Litigation Hold.

Information Technology Regulations

- (a) The Information Technology department will keep all active e-mail on the production server for a 90 day period after the e-mail is generated or received.
- (b) After the 90 day period the Information Technology department will automatically move all active e-mail to online archive.
- (c) The Information Technology department will keep the e-mails that have been archived in archive status for one year. After one year, all e-mail will be deleted.
- (d) The Information Technology department will purge all deleted e-mail 90 days after the deletion date.

400.12 USE OF PHYSICAL TWO -FACTOR AUTHENTICATION

In support of enhanced information security and employee privacy, the City allows the use of physical two-factor authentication (2FA) devices, such as YubiKeys, as an alternative to mobile-based authentication for access to City-managed information systems and services.

- (a) Employees who wish to use a YubiKey in place of their personal mobile phone for authentication must receive written approval from both their Department Director and the Chief Technology Officer (CTO) or their designee. Approval is contingent upon operational need, system compatibility, and adherence to applicable IT security standards.
- (b) Use of a YubiKey must comply with all City of Tolleson Information Technology policies, including access control and data confidentiality protocols. Upon approval, employees are responsible for proper handling, usage, and safekeeping of their assigned YubiKey device.
- (c) A replacement fee will be assessed to the employee if a City-issued YubiKey is lost, stolen due to negligence, or damaged beyond normal wear. The amount of this fee will be determined and communicated by the Information Technology Department and may be subject to change.
- (d) Unauthorized use or sharing of a YubiKey device is strictly prohibited and may result in disciplinary action. Lost or malfunctioning devices must be reported immediately to the Information Technology Department.
- (e) An operating procedure detailing issuance, registration, usage, and return of YubiKeys will be maintained by the Information Technology Department.