City of Yuma
ADMINISTRATIVE REGULATION

Issued by: *Greg Wilkinson*
Authority: City Administrator

SUBJECT:

TECHNOLOGY USE IN THE WORKPLACE

Issued: June 25, 2012

1.0 **PURPOSE:** The purpose of this Administrative Regulation is to establish and provide City of Yuma (City) employees with guidelines on the appropriate and acceptable use of City automated business systems. Employees are to adhere to these guidelines at all times when performing job functions and City business.

The Department of Information Technology Services (ITS) is assigned the responsibility of overseeing and safeguarding the City's automated business environment through the City Administrator.

2.0 **DEFINITION:** The definition of "automated business systems" (systems) for the purpose of this regulation includes any and all City owned voice, video, computer and data systems. Examples of these systems include, but are not limited to:

(a) **Electronic hardware,** such as personal computers and local area network servers, cell/smart phones, Personal Data Assistants (PDA's) desk phones, fax machines, radio equipment, pagers, cameras, printers, scanners, etc.

(b) **System applications,** such as calendar and e-mail, Internet, Social Media sites, voice mail, word processing, security and operating systems, etc.

(c) **Any and all data/information** used, sent, received, or stored on City owned systems or system used to conduct City business.

3.0 **NO EXPECTATION OF PRIVACY:** The City provides employees with the automation tools needed to perform job functions and City business. Employees should not consider any portion of these systems as personal property.

3.1 All information transmitted by and received from, or stored on, City systems is the property of the City. Such systems are subject to disclosure under appropriate state and federal regulations covering public records and should be considered public information, unless otherwise privileged by law.

3.2 Employees should have no expectation of privacy and at all times conduct business in an appropriate and acceptable manner. Highly sensitive or confidential information

(such as personnel and legal materials) should be managed and communicated via a more secure and private method.

3.3 The City may routinely monitor usage patterns, messages and files of its systems to determine whether an alleged violation of law or City policy has or is occurring. Requests for review of usage logs or to request monitoring of technology access must be communicated by the Department Director, City Administrator, or Human Resources Director to the ITS Director.

3.4 User names and passwords are provided to those employees who need access to specific City systems and information. User names and passwords are provided for the purpose of security and information access. Passwords are to remain personal and confidential and employees are prohibited from giving their passwords to any other person or company. Passwords will not be provided to any company to allow access to the City for smart phones, PDA's, or remote access devices.

3.5 Any information from City systems which is saved or stored from City systems is the property of the City.

4.0 PROHIBITED USES: Prohibited uses of City systems include, but are not limited to, anything that:

4.1 violates or infringes on the rights of any other person, including the right to privacy;

4.2 contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material;

4.3 violates City regulations, policies or state or federal laws prohibiting sexual or other unlawful harassment;

4.4 restricts or inhibits other employees from using the systems, or the efficiency of the systems;

4.5 encourages the use of controlled substances;

4.6 intentionally contributes to erasure, deletion or disposal of City information protected under the state of Arizona Public Records Law;

4.7 contributes to excessive personal or non-City/work related business, as defined in Section 5.1, except as permitted on the Employee Bulletin Board, see Section 8; personal or non-City/work business uses include non-City business emails;

4.8 conducts any political activity as defined in Administrative Regulation 3;

4.9 conducts any non-City related fund raising or public relations activities, except as provided for in Employee Bulletin Board;

4.10 encourages the performance of any activity that is prohibited by law (including but not limited to, violation of copyright laws, use of the system to encourage or further

criminal activity or transmission of material, information, or software in violation of any local, state or federal law);

4.11 intentionally sends City confidential materials to unauthorized persons or locations inside or outside of the City;

4.12 subscribes to a mailing list that is non-business related: i.e."joke of the day" or sports updates;

4.13 intentionally sends e-mails with infected file attachments or executes such attachments on the local personal computer;

4.14 uses non-business software including games or entertainment software on the City system;

4.15 intentionally tries to access electronic systems, accounts, applications or data to which the employee is not authorized, except as permitted in Paragraph 5.1;

4.16 uses or attempts to use any privately owned computer and network hardware, software and/or associated peripherals on City systems;

4.17 uses City loaned equipment for personal business

4.18 loans out City owned equipment;

4.19 intentionally accesses pornographic or sexually oriented information/sites; or

4.20 intentionally pirates computer software or violates any copyright laws;

4.21 unauthorized access to City systems or the corruption of City information systems by use of hacking tools or malicious computer code;

4.22 allows third party agencies or individuals to connect equipment to City systems without consent of ITS;

4.23 uses system resources for video streaming or streaming radio/audio unless required for job function and approved by employee supervisor with concurrence from ITS. Video streaming (ie You Tube) will only be used for City business.

5.0 **INTERNET USAGE:** Not all sources on the Internet provide accurate, complete, or current information. The City assumes no responsibility for the content and/or accuracy of information residing on other systems.

5.1 The City provides Internet access to employees for use in performing job functions. The City may allow employee access to the Internet for incidental use, but employee use may not exceed one hour in any pay period. This one hour of permitted use is still subject to the prohibited uses outlined in Section 4.0. Exceptions are outlined in Section 5.7.

5.2 The Internet may contain materials of a controversial nature. Employees are responsible for the material that s/he accesses, sends and receives and what is contained or stored on the systems assigned them.

5.3 Alternate Internet Service Provider connections to the City's internal network (i.e. personal dial-up Internet accounts) are not permitted unless expressly authorized by ITS and properly protected by an appropriate security device.

5.4 Using the Internet to download files or receiving such files via an e-mail attachment can cause serious damage to the City's systems because of the potential harm viruses can cause. All downloaded data from the Internet must be virus scanned with anti-virus detection software provided by the City.

5.5 To prevent instability on City systems, downloading of software (i.e. updates, shareware, freeware, etc.) is prohibited unless previously reviewed and approved by ITS. All software must be fully tested for stability and to insure that it is virus free before being loaded to City systems. Also, all software is to be properly purchased and registered with the software vendor and be on record with ITS to avoid copyright liability and ensure asset inventory.

5.6 The City recognizes that certain departments within the City have a business need to access sites that would otherwise be inappropriate. Filtering tools allow the City to restrict certain types of Internet sites while allowing exceptions to the restriction. Social Media use and visiting certain aspects of Social Media are outlined in AR15.

5.7 Educational use of computers is allowed for City approved courses and with the approval of the Department Director. Supervisors may grant flex scheduling for employees to complete assignments for City approved courses or approve time to attend online meetings required for the course. It is the responsibility of each employee to schedule flex time with their supervisors in the completion of course work on City time and equipment. Employees must utilize personal email accounts to conduct correspondence concerning education pursuits. All other aspects of this regulation shall apply.

6.0 **E-MAIL:** The City provides e-mail accounts and services to employees for use in performing job functions. Employees should limit use of email to City business only, unless submitting a personal request for publication to the employee electronic bulletin board (see Section 8 of this AR for applicable rules). If an employee receives material that is non-City business related s/he may forward the e-mail to a personal account and must delete the correspondence from the City system.

6.1 City employees should keep in mind that anything sent or posted over the City's email system will reflect upon the City's image. City employees must be aware that any communication transmitted electronically can be re-sent or forwarded, intentionally or accidentally, by the recipient to others. All e-mail messages and attachments must be business-like, courteous, civil and written with the expectation that they could be made

public at any time, therefore, must not contain inappropriate, illegal or offensive material or statements.

6.2 If an employee forwards a non-City business related e-mail to a personal account all references to the City must be deleted before further forwarding the e-mail. This includes but is not limited to job titles and e-mail addresses present in the e-mail's forwarding history.

6.3 E-mail messages sent or received, both internally and externally are potentially subject to the Public Records Law and therefore, should not be considered personal or confidential. This also pertains to City business conducted from personal home computers.

6.4 The City reserves the rights to access employee e-mail messages to determine whether an alleged violation of law or any other City regulation or policy has occurred.

6.5 If an employee receives inappropriate or offensive messages, s/he should report the situation to the ITS Department for assistance in investigating the source of the messages, as appropriate, as well as assistance with proper disposal.

6.6 Confidential information (such as personnel or legal materials) should be communicated via a more secure and private method.

6.7 E-mail attachments are scanned by the City's e-mail virus protection software. It is still the responsibility of employees to be cognizant of any unexpected or suspicious e-mails from known or unknown sources and to report these to ITS immediately, before opening the attachment.

6.8 FLSA requires Non-exempt employees to be compensated when working on city business outside of regular scheduled work hours. FLSA applies to all areas of city business including but not limited to use and operation of electronic media such as email, phones, social media etc. Use of these systems by non-exempt employees outside of normal work hours requires the approval of the supervisor.

7.0 **VOICE AND DATA SYSTEMS:** The City finds it advantageous to utilize various systems, such as desktop computers, notebooks, laptops, and other mobile devices to perform job functions and conduct City business. Connectivity of these systems to City Local Area Networks (LAN) via the City's Wide Area Network (WAN) may occur, therefore, employees should not assume they are working in a stand-alone, single environment.

7.1 All such hardware, software and data generated by and stored in such systems remains the property of the City and are subject to inspection by the City.

7.2 In an effort to insure standardization of City systems, facilitate information exchange across City systems and assist in providing support, employees are prohibited from installing or connecting any non-City owned products on City systems, unless authorized by ITS.

7.3 In an effort to protect the integrity of the City's network systems and the data that may be stored on personal computers, all City personal computers are equipped with anti-virus software. This virus protection software must be kept operational; no matter what effect it has on the computer system's performance. Anti-virus software installed on City systems shall not be disabled, except in situations deemed appropriate by ITS.

7.4 If a virus is introduced on any City computer or network due to an employee intentionally disabling the anti-virus software, appropriate disciplinary action shall be taken.

7.5 Employee's are responsible for immediately reporting the loss of any device that can potentially access City information systems to ITS Help Desk during working hours or to ITS recall phone after working hours. Immediately is defined as when the employee becomes aware that the device is missing. ITS will temporarily disable access until further investigation can be performed.

8.0 **EMPLOYEE ELECTRONIC BULLETIN BOARD**: An electronic employee bulletin board is available to City employees via the City's internal private network (Intranet). The bulletin board is not available to the general public from the world wide-web (Internet). The purpose of the bulletin board is to centralize information that may be of interest to City employees. It is also intended to be fun and informative. When submitting publications to the bulletin board:

8.1 All publications must be business-like, courteous, civil and written with the expectation that they could be made public at any time and, therefore, must not contain inappropriate, illegal or offensive material or statements.

8.2 Advertisement of employee owned or employee operated commercial or for-profit businesses and products are not permitted.

9.0 **VIOLATION AND ENFORCEMENT OF POLICY:** Violations of this policy may result in disciplinary action, up to and including dismissal from employment. Criminal or civil action against employees may be appropriate where laws are violated.

9.1 While basic responsibility and accountability must begin with the employee, the department directors, managers and supervisors are responsible to insure employees' understanding and compliance with this regulation.

9.2 When an instance of non-compliance with this policy is discovered or suspected, the department shall proceed in accordance with departmental and City personnel policies.

9.3 Suspension of service to employees may occur when deemed necessary by the department director when this policy is violated.

9.4 Discipline may be appropriate for non-compliance with this policy.

9.5 Any action by City or non-City personnel which could jeopardize the security of any City system should be reported immediately to a supervisor and ITS for immediate action and assistance.

9.6 It shall not be a violation of this Administrative Regulation if the activity prohibited is specifically authorized by the City Administrator, City Attorney or Police Chief.

10.0 <u>CITY'S RIGHT TO WAIVE OR AMEND</u>: When it is deemed in the best interest of the City to do so, the City Administrator or designee may waive or amend any portion of this Regulation not in conflict with the Personnel Rules, City Charter, City Ordinance, or Arizona state or Federal law.