City of Phoenix

ADMINISTRATIVE REGULATION	A.R. NUMBER 1.63 Revised
	FUNCTION Information Technology Page 1 of 6
SUBJECT **ELECTRONIC COMMUNICATIONS AND INFORMATION ACCEPTABLE USE**	EFFECTIVE DATE June 26, 2014
	REVIEW DATE

Transmittal Message

Email questions about this Administrative Regulation (A.R.) to the Information Technology Services, Information Security & Privacy Office at ISPO@phoenix.gov.

I. PURPOSE

The purpose of this A.R. is to govern the acceptable use of City of Phoenix (City) information systems, electronic communication channels, and Internet access in support of City business requirements. The elements in this A.R. provide measures that

- Protect the confidentiality, integrity, and availability of City information and help preserve the public trust
- Increase the City workforce's effectiveness by promoting efficient, clear, and accurate electronic business transactions and communications
- Minimize security incidents
- Emphasize the public record aspects of electronic information, and
- Protect the City from legal liability.

II. SCOPE

This A.R. applies to all members of the City workforce.

III. DEFINITIONS

- City business – All work performed on an electronic device that has a direct relation to the City's operation and activities. City business includes any work performed where non-transient public records may be created, transmitted, or stored using a personal mobile device.

- City workforce – Anyone authorized to access City information systems and information including, without limitation, City employees, non-City employees, business partners, contractors, volunteers, and temporary workers.

- Criminal Justice Information (CJI) – Data provided by the Federal Bureau of Investigation (FBI) for law enforcement agencies to perform their mission and enforce the laws. CJI includes biometric, identity history, person, organization, property, and case/incident history data.

- Electronic communications – Any software or electronic information or telecommunications system including email and voice mail systems, instant and text messaging systems, facsimile machines, video-conference devices, software for net-meetings, webcasting, and other collaborative Web technologies.

- Information system – Any hardware, software, or electronic system that the City owns, operates, maintains, or provides and authorizes for use in storing, accessing, analyzing, and manipulating business information. These systems include business application systems, databases, Internet and intranet sites, file servers, document management systems, and their infrastructure.
- Personal device – Any electronic storage or multi-function computing and communications device capable of hosting a broad range of applications for both business and consumer use that is not owned by the City, but owned or provided by City workforce. Personal devices include, but are not limited to USB sticks, removable hard drives, personal digital assistants (PDAs), smartphones, and tablet, pad, desktop, and laptop computers.

IV. ROLES and RESPONSIBILITIES

- Department Heads are responsible for ensuring their department complies with this A.R.
- The Chief Information Security Officer or designee is responsible for interpreting and revising this A.R.
- The City workforce is responsible for understanding and complying with this A.R and for annually acknowledging their compliance with City information security policies.

V. POLICY STATEMENTS

1 **City Workforce Accountability**. All members of the City workforce are accountable for the security of their user IDs and passwords, and for all actions performed by their computer accounts. City workforce members may not use another's user ID and password, nor allow another to use their user ID and password.

2 **Privacy Expectations**. The City workforce has no expectation of privacy for any electronic information created, received, stored in, or transmitted on the City's electronic property or electronic communication systems.

In accordance with Arizona's Public Records Law, the public may request all information made or received by City workforce in performance of their jobs. The City workforce must consider all information, including email and City information residing on personal devices, open to public view unless the Law Department determines there is a specific legal confidentiality requirement.

3 **Use of Personal Devices**. As described below, the City workforce may use personal devices for work involving information classified as public. Reference: s1.9 Information Classification Standard.

City workforce members performing any work on personal devices are encouraged to connect to the City's network using the City's remote access facility to best protect City information. To help ensure compliance with Public Records Law, the City workforce should not store any City information on a personal device or system.

While City workforce members may use personal devices to access their City email as stated below, they should not conduct City business using personal email accounts.

City workforce members may not use personal devices for work involving any personal identifying or restricted City information that may result in a critical breach of information security. Reference: A.R. 1.90 Information Privacy and Protection.

The City workforce may not use personal devices to access Criminal Justice Information unless specifically authorized by the City's Criminal Justice Information Services (CJIS) Officer. The CJIS Officer must

approve and authorize any access, processing, storage, or transmission of Criminal Justice Information using personal devices.

3.1 Use of Personal Devices for Messaging. The City workforce may use personal devices, such as smartphones for telephone, texts, and email related to City business. While the City workforce must comply with all other provisions in this A.R., no additional approvals are required.

3.2 Use of Personal Devices for Messaging and Offline Work. The City workforce may use personal devices, such as pad and/or tablet computers for texts, email, and work related to City business without connecting to the City's network. This includes accessing email via a web browser. While the City workforce must comply with all other provisions in this A.R., no additional approvals are required.

3.3 Use of Personal Devices Connecting to City Network. The City workforce may use personal devices, such as pad, tablet, laptop, or desktop computers to connect to the City's network with approval from their department's information security liaison and with the understanding that the City may require City-provided and monitored management software to ensure compliance with City policies.

4 Personal Use. The City workforce may use City information systems for incidental personal use as long as it

- Consumes only a minimal amount of computer system resources or staff time
- Does not interfere with productivity or any business activity
- Does not cause the City to incur additional costs
- Does not require repeated and ongoing use or registration of their City email account, as City workforce members should not use their City email address as their primary personal email account
- Does not violate any City A.R. or standard, or any applicable law or regulation, and
- Would not adversely affect the reputation of the City, its citizens, or its employees.

5 Unacceptable Use. The City workforce must use City information systems in compliance with this A.R. Examples of unacceptable use include, but are not limited to the following:

- To upload, transmit, display/view, or store offensive, derogatory, defamatory, improper, harassing, sexually explicit, pornographic, obscene, vulgar, or profane messages or materials that violate or infringe in any way upon the rights of others, or that are unlawful, threatening, abusive, defamatory, or otherwise objectionable, even in a joking manner
- To access restricted-content Web sites, such as sexually explicit, pornographic, racist, or hate sites

  City workforce members must immediately disconnect from any Web site they have inadvertently connected to that contains sexually explicit, racist, violent, or otherwise inappropriate content. The ability to connect with a specific Web site does not in itself imply that the City workforce is permitted to visit that site.
- To copy or disseminate copyrighted materials, such as articles, movies, music, or computer software, in a manner that is inconsistent with applicable copyright laws or licensing agreements
- To use their City email account to post or email their personal information on public Web sites, blogs, or other external destinations, including online auctions

  Members of the City workforce should not appear to be representing the City of Phoenix when

conducting personal business.

Only authorized and approved members of the City workforce may write, publish, or post official City information on social media sites.

- For personal gain or for personal businesses
- For political purposes, including campaigning and voting, except as provided in A.R. 2.16 Political Activity – Time off to Vote
- To use unapproved peer-to-peer or other software, such as LimeWire, BitTorrent, or KaZaA, or
- To transmit or forward chain letters, third-party advertisements, or third-party solicitations, or to set up forwarding agents that automatically forward email to personal or other external email accounts.

6 **Required Training**. The City workforce must complete all applicable information security awareness training within the timeframes that the City establishes. This includes, but may not be limited to new hire and annual training.

7 **Security Software**. The City workforce must not disable or circumvent any software or controls intended to safeguard City information systems.

8 **Unattended Devices**. The City workforce must appropriately protect all unattended information systems and promptly report any suspicious activity that may affect information security, or the loss or theft of a device containing City information to their department's information security liaison.

9 **Authorized Software**. The City workforce must use only City-authorized software on City-owned devices. The City workforce may neither use nor distribute unauthorized software in the course of performing City business. Reference: A.R. 1.86 Legal Use of Software.

10 **Copyrights and Licensing**. The City workforce must always comply with all applicable copyright and license requirements. Reference: A.R. 1.86 Legal Use of Software.

11 **Records Management**. The City workforce must comply with all records retention policies and schedules. The City workforce must not delete and/or modify any electronic records in a manner that violates their approved retention periods and/or any other legal requirements. For example, members of the City workforce must not empty their email system trash or modify activity logs. Reference: A.R. 1.61 Records Management Program.

12 **System Use**. The City workforce must use City information systems and protect City information in accordance with all A.R.'s and standards. Reference: A.R. 1.84 Information Security Management.

13 **Ownership**. The City owns all information residing on its information systems. Upon termination of City employment, contract, or agreement, City workforce members must return all equipment, software, and information, whether in electronic form or otherwise.

VI. PRIVACY AND MONITORING

The City reserves the right to monitor systems, electronic communications, and usage to support operational, maintenance, auditing, security, and investigative activities, including enforcement of this policy, legal requests, public record requests, and to help ensure and to verify compliance, confidentiality, integrity, and availability of information systems used to conduct City business. This A.R. does not prohibit technical staff from monitoring departmental workstations and servers for the purpose of maintaining overall system reliability, availability, and security. Unauthorized accessing, monitoring, or reading of electronic communication systems or their contents violates this City policy.

City departments are responsible for handling public requests for their electronic information, including email messages, and for working with their legal, human resources, City Clerk, and Public Information Office representatives, as needed, before making the records available to the public.

City Department Heads may approve initiating an investigation of their workforce's compliance with this A.R. and must coordinate the investigation with the Human Resources (HR) Director and the department's legal representative. The HR Director may authorize access and monitoring of email based on Department Head requests. If authorized, the HR Director will forward requests to Information Technology Services, or the Police Department for Police staff, to process email requests and maintain them. The HR Director may consult with the Chief Information Officer for technical advice and/or assistance in the course of a lawful investigation.

VII. COMPLIANCE

All City workforce members agree to abide by and comply with this A.R. The City workforce must consider all information, including email and City information residing on personal devices, open to public view unless the Law Department determines there is a specific legal confidentiality requirement. The City Auditor Department may conduct periodic audits to evaluate compliance with the responsibilities set forth in this A.R.

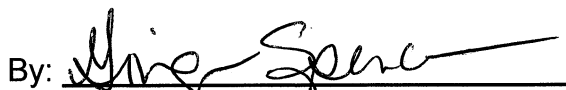
A violation of this A.R. may result in disciplinary action, up to and including termination of employment. In the case of contractors and temporary workers who violate this policy, the City may revoke any and all system access and use privileges and terminate the third-party contract(s).

All exception requests must follow the authorized waiver procedure.

VIII. RELATED POLICES, STANDARDS AND PROCEDURES

A.R. 1.61 Records Management Program
A.R. 1.73 Control of Communication Services and Systems
A.R. 1.84 Information Security Management
A.R. 1.86 Legal Use of Software
A.R. 1.90 Information Privacy and Protection
A.R. 1.91 Information Privacy and Protection Supplement – Data Shared With Third Parties
s1.1 Virus Protection
s1.2 Web Filtering
s1.3 Identity Management
s1.4 Remote User Access
s1.5 Password Management
s1.7 Media Retention/Removal
s1.8 Internet Email Content Security
s1.9 Information Classification
s1.10 Collaborative Web Technologies Usage
s1.2.1 Requesting Access to Blocked Web Sites
b1.3 Waiver Standard

ED ZUERCHER, City Manager

By: 
Ginger Spencer
Special Assistant to the City Manager

CITY OF PHOENIX

ELECTRONIC COMMUNICATIONS AND INFORMATION ACCEPTABLE USE

CITY WORKFORCE RECEIPT

This form must be signed by each current and new member of the City workforce.

I acknowledge that I have received A.R. 1.63, Electronic Communications and Information Acceptable Use. I recognize that as a user of City information, electronic communications, and computer systems I am responsible for following the provisions outlined in this policy. I understand that if I am found to be in violation of this written policy, I may be subject to disciplinary action.

Name (printed) _____

Signature _____ Date _____

c: Copy to individual member of the City workforce

Original to department file