Administrative Regulations

AR127 – Electronic Communications

By: Don Thelander, Network Security Director, x22712; Robert Fisher, IT Director, x27688 and Shannon Tolle, Communications Director x27631

Responsible Department:
Information Technology, Main ext. x22622

Effective Date:
10/21/2002

Approvals:
Fritz Behring, City Manager for BB
Brad Hartig, Chief Information Officer BH

Date Approved:
08/01/2014
09/05/2013

1. PURPOSE

1.1. This Administrative Regulation ("AR") clarifies the City of Scottsdale's policies governing the use of electronic communications and the means of transmitting them, i.e., electronic communication systems, including but not limited to: email, voice mail, telephone, instant messaging, smartphones, electronic calendar, wireless, Internet and intranet technologies.

2. APPLICABILITY

2.1. This AR applies to all staff at the City of Scottsdale. The definition of "staff" for this AR includes all employees, contract staff and volunteer staff. (Note: AR #165 "Internet Use," remains in effect. It is supplemented, but not replaced, by this AR).

3. POLICY

3.1. The electronic communication systems are part of the working tools used by this organization to serve the Scottsdale community more effectively. The use of electronic communications is a privilege, not a right and the use of electronic communication systems for non-business matters must be limited to emergency use only. (Examples: brief telephone call to check on welfare of a family member or to schedule a doctor's appointment). Any questions regarding appropriate use of these resources should be directed to the employee's supervisor. The employee's supervisor, together with Human Resources staff, will make the ultimate decision as to the acceptability of use. Each employee is responsible for any information or message that he or she generates and/or distributes via electronic communication systems.

3.2. The city's email system allows users to submit a personal photograph that is visible to other internal users. Photos submitted for this purpose must be of the employee in a setting and attire that is appropriate for the workplace.

3.3. Examples of prohibited uses:

- Automated blanket forwarding of city email to personal email boxes on home computers or personal phones. (Except for Information Technology authorized applications or services.)
- Unauthorized downloading and distributing of copyrighted materials.
- Unauthorized reading, deleting, copying, modifying, or printing of electronic communications of another user.
- Soliciting for political, religious or other non-business uses.
- Sending or forwarding unsolicited junk mail, chain letters or mass mailings.
- Using, accessing, transmitting or forwarding religious or political messages, material of an obscene, threatening, demeaning, harassing or otherwise offensive nature, whether in words or images that would be either illegal, prohibited or inappropriate under AR #333 "Anti-Discrimination and Non-Harassment," or any provision of Chapter 14 of the City Code ("Human Resources Management").
- Non-compliance with established policies described in AR #128 "Personal Electronic Communication Device Usage."

3.4. City Property and Public Records Requests: All hardware, software, databases, spreadsheets, files, documents and all messages generated on, or handled by, the city's electronic communication systems (including "backup" copies) are the property of the City of Scottsdale and may be disclosed as part of a public records request. Any information and/or data created, received, stored in, or sent from the city's electronic communication systems may be reviewed by authorized employees, such as a supervisor, the City Attorney's Office, Human Resources personnel or Information Technology personnel, in the course of their official duties.

3.5 Retention: Public records retention and disposition schedules are established by state law and are based on a record's informational content, not on its format. The City of Scottsdale creates "backup" records of electronic mail on a daily basis. The sole purpose of creating these "backups" is to restore electronic records in case of system failure, not for purposes of retention of public records. The "backups" are retained for the limited time period required by law for "backup data."

This retention period is different from the time period the document itself must be retained. It is the responsibility of each city division and each employee to retain any electronic communications, depending on the nature and content of the document, as required by the public records retention and disposition schedules. Records retention and disposition schedules that apply to city records are available through the City Clerk's Office. Refer to AR #295 "Citywide Records Management Program."

Instant messaging (IM) is not backed up or logged so, therefore, should only be used for communications that can be considered casual or transitory. This means that any outgoing instant message should only be used for communications that are useful for a short period of time and do not reflect final city decisions. For communications that produce records with lasting value, other options should be considered, such as email. If an IM is received from an outside party that would be classified as a public record, the receiving party must forward a copy to their

city email address so the record can be preserved in accordance with the city's public record retention schedule.

3.6 Sanctions: Violations of this policy may result in revocation of privileges relating to electronic communications, disciplinary actions pursuant to Chapter 14 of the Scottsdale Revised Code and other possible legal consequences. A single incident in violation of this AR may be grounds for disciplinary action, up to and including dismissal.

4. PROCEDURES

4.1. New Hires (Includes Contract Workers): The city's Information Technology department requires all new hires or existing employees receiving a new network User ID, to attend a technology orientation. The purpose of this training is to familiarize new users with the security policies regarding network access, electronic communications policies, Internet use and a general technology overview. The new user will get their network ID and user password for the first time during this session, along with setup instructions and appropriate use of email. A short overview of the city's intranet is also presented. Employees needing Internet access for business use will need to submit that request along with their supervisor's approval, to the IT Helpdesk, or the Information Technology network security director.

4.2. Employee Termination: When an employee leaves the city, the employee's supervisor is required to submit a "work order" using the city's IT Work Order Portal to disable the employee's IDs within the network. This includes email account, server account, Xpressions (voice mail) account, and any special IDs or accounts that are set up in the employee's name. If a situation occurs which requires immediate termination of an employee, the employee's supervisor can contact the city's network security director, or designee, by telephone to request an immediate disabling of the employee's IDs. This phone request should be followed up with an email in order to document the request. Ninety (90) days after the employee's IDs are disabled; all data associated with that employee that is still on the network will be purged from the system. The employee's PC will also be wiped clean before it is assigned to another city staff member.

4.3. Monitoring: The City of Scottsdale reserves the right to monitor the content of electronic communications, without notification. Electronic communications may be monitored to support operational, maintenance, auditing, security and investigative activities.

- If a manager has reason to believe that an employee, under his/her direct supervision, may have engaged in any prohibited behavior with, or inappropriate use of, electronic communications, it is the manager's responsibility to contact the human resources director, or designee(s), who will guide the manager through the process of documenting the allegations. The decision of whether or not to monitor the employee's electronic communications, and/or conduct a search of the employee's electronic files shall be subject to the prior approval of the Human Resources Director, or designee(s). For Police investigations of staff regarding potential criminal activity, or Police internal investigations, searches may be initiated directly by the Police Department with notification to Human Resources provided at an appropriate stage of the investigation.

- If a decision is made to monitor and/or research electronic communications, the requestor will send a written request to Information Technology for their staff to provide the technical assistance required. Information Technology staff, however, will be excluded from any examination of content of the electronic communications, which will be subject only to review by the Human Resources Director, or designee(s); manager(s) with an official need to know the information and such members of the City Attorney's Office, who may be consulted to provide legal advice and assistance.

5. RESPONSIBILITIES

5.1. Employee: It is the responsibility of every employee to use the city's electronic communication systems responsibly in the interest and furtherance of the public's business. All employees are required to read and understand all policies and procedures regarding the use of the city's electronic communications prior to being assigned logins and passwords. These policies and procedures can be found in the following city documents:

- AR 128 - Personal Electronic Communication Device Usage
- AR 136 - Network and Computer Security
- AR 165 - Internet Use
- Information Technology Security Policy

5.2. Management: If a manager has reason to believe, or it has been reported to the manager by another staff member that an employee under his/her direct supervision may have engaged in any prohibited behavior with, or inappropriate use of, electronic communications, it is the manager's responsibility to contact the human resources director, or designee(s), who will guide the manager through the process of documenting the allegations.

6. OVERSIGHT/REVIEW

6.1. Audit Logging: The network generates logs that track usage of computer resources. These logs are utilized by IT security and network personnel to ensure policies are being followed, the network is being properly managed and maintained, and security violations are being tracked and reported.

6.2. Email Limitations: Sending large attachments through the city's email systems negatively affects overall efficiency. To keep the city's system running smoothly, Information Technology has placed a system limit on the size of outgoing and incoming email messages. Current system limits and additional information on how to reduce file sizes may be found on the IT intranet website. In cases where larger files must be sent, Information Technology provides a service that allows for the secure transmission of files without affecting the city's email system. Call the IT Helpdesk (ext. 27827) to receive more information about this service.

6.3. Security: Security policies are listed under "Network and Computer Security" Administrative Regulation (AR #136). Anyone that uses the city's electronic communication systems will be required to review this regulation. Administrative Regulations are available on the city's intranet.

6.4. Network Connectivity: Each time an employee logs onto their workstation on the City's network, the following message is displayed:
"This system is City property. By accessing and using this system, you are

consenting to monitoring by the City of any data or transmissions. Unauthorized use of this computer system may subject you to disciplinary and/or legal action."

7. DEFINITIONS

7.1. Electronic Communication Systems: Email, voice mail, telephone, instant messaging, smartphones, electronic calendar, wireless, Internet and intranet technologies.

7.2. Network User ID: The designated unique sign-on an employee is required to use to access the city's network and computer systems. This ID is always required along with a unique employee generated password.

7.3. User Password: A password is a confidential string of characters which is presented as part of an authentication process to verify an identity. User passwords are required to access all city networks and systems, and will normally require the employee to change them every ninety (90) days or less.

7.4. IT Helpdesk: The Information Technology Helpdesk (ext. 27827) provides assistance, problem resolution and work-order submission for computer, networking and telephony problems.

8. RELATIONSHIPS TO ADOPTED POLICIES AND ORDINANCES

8.1 AR 128 - Personal Electronic Communication Device Usage

8.2 AR 136 - Network and Computer Security

8.3 AR 165 - Internet Use

9. LINKS TO SUPPORTING DOCUMENTS

9.1. AR 128 - Personal Electronic Communication Device Usage

9.2. AR 136 - Network and Computer Security

9.3. AR 165 - Internet Use

10. REVIEWED/AMENDED DATE(S) AND NOTES ON SIGNIFICANT CHANGES

10.1. Each time the AR is reviewed, the review date should be added. For all substantive updates, a brief explanation of the sections changed and the rationale for changes should be added as a guide to the reader.

Original Effective Date: 10/21/2002

Review Date: 08/01/2011 - Updated entire document including migration to the newly adopted AR format.

Review Date: 09/05/2013

- Updated City Manager and owner information
- Section 1.1 - Deleted introduction paragraph due to irrelevance
- Section 1.1 – Added reference to instant messaging
- Sections 3.4 and 3.5 – Combined city property and public records sections to remove duplication

- Section 3.5 – Added wording pertaining to the appropriate use of instant messaging
- Section 6.2 – Added wording pertaining to transferring large files
- Section 7.3 – Removed irrelevant information