


AR136 – NETWORK AND COMPUTER SECURITY

	Responsible Department:	Effective Date: 02/13/2006
	Approvals: <u>DER</u> David E. Richert, City Manager <u>BH</u> Brad Hartig, Executive Director-IT/CIO	Date Approved: <u>12/16/11</u> <u>11/4/11</u>

1.0 **PURPOSE**

- 1.1. Computer information systems and networks are an integral part of conducting business at the City of Scottsdale. The City makes a substantial investment in human and financial resources to create and maintain these systems.
- 1.2. This Administrative Regulation ("AR") specifies security policies and procedures that are to be reviewed and practiced by all staff that access the City's computer information systems and networks. The definition of "staff" for this AR includes all employees, contract staff and volunteer staff.

2.0 **APPLICABILITY**

- 2.1. This AR has been established in order to:
 - Make all City staff aware of their responsibilities regarding security for the City's information systems, communications networks, and data.
 - Protect the public investment.
 - Safeguard the information (data) contained within these systems.
 - Reduce potential business and legal risks.
 - Protect the public trust and ensure the confidentiality of the City's computer information systems and networks.
 - Communicate to City employees and other staff how Arizona state law affects the use and access of information systems and networks.

3.0 **POLICY**

- 3.1. **System Access/Data Protection:** All City employees are responsible for the technology equipment assigned to them and for the security of any data to which they have access. Regularly changing and safeguarding passwords, as well as not leaving data in unsecured locations, are methods of safeguarding City information systems and data. Employees and other staff must protect City data by limiting its use for only official activities by authorized users.
- 3.2. **State Law:** Computer fraud and misuse is a felony under Arizona state law (Arizona Revised Statute Section 13-2316). Intentionally accessing, altering, damaging or destroying without authorization or **EXCEEDING AUTHORIZATION OF USE** of any computer system or computer network or any computer software, program or data contained therein, constitutes computer fraud.

AR136 – NETWORK AND COMPUTER SECURITY

- 3.3. **Business Use Only:** The City's information systems are for the legitimate business use of City staff, and other authorized personnel, to conduct City business.
- 3.4. **Passwords:** Passwords are critical to the security of our network and computing systems. Individual passwords are not to be given to, or shared with others. Each person requiring access to the network or computing systems must acquire proper authorization to obtain their own User ID and password. Passwords must be a combination of three of the following groups:
- Upper case letters, lower case letters, numbers, or punctuation characters (words from the dictionary or sequential or repetitive numeric sequences should not be used)

For systems that do not currently support these "strong" password requirements, such as Voice Mail, select a password that will not easily be guessed. (i.e., do not use street addresses, phone numbers, numeric sequences, etc.)

- 3.5. **Locked Workstations:** All workstations and servers are to be "locked", logged off, or powered off by the responsible staff member whenever the workstation or server is left unattended (i.e., whenever you leave your immediate work area). All workstations and servers will utilize a password protected screen saver that is automatically invoked after no more than ten (10) minutes of non-activity.
- 3.6. **Anti-Virus Software:** All City workstations employ an approved anti-virus screening program. If the screening program detects a virus, staff must immediately notify the Information Technology ("IT") Support Desk. Users will NOT attempt to eradicate a virus or use the affected machine until Information Technology personnel have been notified so they may document and address the problem. Do NOT turn the workstation off unless directed to do so by IT Support Desk staff.

It is the responsibility of each staff member to use reasonable care to prevent the introduction of viruses into their systems and the possible infection of other systems. If you receive notification from the anti-virus software that your personal computer has an infection, immediately contact the IT Support Desk (ext. 27827). All City of Scottsdale staff must help ensure that City owned computers, electronic files, and electronic media used to conduct City business are protected from computer viruses. **Staff is not permitted to override the virus detection software installed on any system.**

Users that request remote access to the City network, utilizing their personally owned home computer(s), must agree to install and keep current, at their own expense, anti-virus software on those computer(s) to help safeguard the City's network.

- 3.7. **Confidentiality and Privacy:** All messages (web, email, etc.) sent over City networks and computing systems are the property of the City of Scottsdale. To properly maintain and manage these resources, management reserves the right to examine all data stored in, or transmitted by, these systems and related infrastructure components. Staff should have no expectation of privacy associated with the information they store in or send through these systems.

Management reserves the right to examine archived electronic mail, personal file

AR136 – NETWORK AND COMPUTER SECURITY

directories, hard disk drive files, and other information stored on any City of Scottsdale network or computer system. This examination is performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of all computer information systems.

- 3.8. **Electronic Monitoring:** To better protect City's work environments, individuals may be subject to electronic monitoring while on City of Scottsdale premises. This may include, but is not limited to, network monitoring and video surveillance. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms and locker rooms, no electronic monitoring will be performed.
- 3.9. **Workstation Software Standards:** Basic workstation setup standards are to be maintained and documented by the IT Technology Infrastructure group. Only authorized software applications and utilities may be loaded onto user workstations. IT technicians or divisional/departmental "Technology Partners" will normally perform installation of City standard applications. Authorized software also includes items purchased by operating departments with IT concurrence.

Installing unauthorized applications is not permitted as they can impact the performance of the workstation and potentially circumvent security controls implemented by the City. Examples of unauthorized applications include any personally owned software as well as including games, screen savers, etc. Unauthorized applications will be removed and the user subject to possible disciplinary actions.

- 3.10. **Remote Access:** Remote access to the City's network and computer information systems is available for conducting appropriate business and related support activities. Several methods of access may be used depending on individual requirements, including:
- Webmail (Web based Outlook)
 - VPN (Virtual Private Network)

VPN access requires approval from the requestor's Executive Director. The requesting division is responsible for purchasing any required hardware or software. More information can be found on the Information Technology Intranet web site.

Users that request remote access to the City's network, utilizing their personally owned home computer(s), must agree to install and keep current, at their own expense, anti-virus software on those computer(s) to help safeguard the City's network.

- 3.11. **Portable Equipment Use:** The City of Scottsdale provides selected members of its workforce with portable computer equipment so that they can perform their jobs at remote locations. The information stored in these computers is City of Scottsdale property, and like the equipment, it must be returned to the City of Scottsdale at the time workers are no longer employed by the City. The information belongs to the City of Scottsdale and it can be inspected or used in any manner and, at any time, by the City of Scottsdale.

Theft of portable computers and other electronic devices is commonplace today

AR136 – NETWORK AND COMPUTER SECURITY

due to their value and small size. Workers using these computers must make back-ups of all critical information prior to taking out-of-town trips. These back-ups should be stored elsewhere than the portable computer's carrying case. This precaution supplements the periodic back-ups that must otherwise be made. Staff must keep City of Scottsdale portable computers in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe. Staff in the possession of portable laptop, notebook, tablet, and other transportable computers containing sensitive City of Scottsdale information must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler as hand luggage. When not used within a docking station, laptop computers in non-secure areas shall be locked using a cable lock or stored within a locked drawer or cabinet.

- 3.12. **Personal Equipment Use:** The City offers a limited capability for personally owned devices to connect to the City's email system. Use of personal computing devices such as Cellular phones with data connectivity, Smartphones, Blackberry devices, iPad, iTouch, PDAs, and other mobile and portable computing devices personally owned by City staff, that establish connectivity to the City network through the Internet, are subject to the following:

Active non-business use of personal electronic equipment during work hours (e.g. cell phones, smartphones, computers, etc.) will be limited to occasional emergency use and will not disrupt or interfere with your, or others, normal workplace duties. For more information, please refer to AR128 Personal Electronic Communication Device Usage.

- 3.13. **Acquisition of Hardware and Software:** All hardware, software, and technology solutions acquired for use on City of Scottsdale computer systems and networks will be obtained through established purchasing procedures and must have prior concurrence from the IT Technology Director. All items will conform to the standards established by IT. These standards may be amended from time-to-time, subject to the approval of the City's Executive Director –IT/CIO with the consensus of the IT Technology Director and the Network Security Engineer. This includes purchase, lease, rental and trial use hardware and software. All items must have concurrence, in writing, from IT prior to acquisition and will follow the process outlined in the IT Procurement Directive.

Information Technology is responsible for the tracking of software licenses for software used on City of Scottsdale computer systems. IT staff (or staff authorized by IT) will retain the actual software media. This is to ensure that unauthorized use or duplication of the software does not occur and that its use is limited to the extent allowed in the license agreement from the vendor or manufacturer.

- 3.14. **Non-City Owned (Personal) Hardware and Software:** No personally, or third-party, owned hardware or software will be directly connected to, or installed on, City systems or networks. This includes, but is not limited to, computer accessories (e.g. mice, digital cameras, scanners), flash drives, networking equipment of any kind, digital music and pictures, games, etc.
- 3.15. **Hardware Installation/Relocation:** The IT Division is responsible for maintaining a large inventory of computing, networking, radio, and telephony equipment within the City. To help ensure proper tracking and accuracy of this

AR136 – NETWORK AND COMPUTER SECURITY

inventory, only IT technical staff (or staff authorized by IT) is authorized to install, relocate, or remove any equipment of this type. Any desired relocation of this type of equipment will be scheduled in advance via the IT work order system and is subject to the approval and scheduling of the IT Technician Manager.

- 3.16. **Phone System:** The City's phone system and voice mail systems are specialized information systems and must also be protected. Staff must never enter special numbers and/or codes into the phone system at the request of anyone claiming to be from the phone company or an IT technician. Staff should refer any related questions to the IT Support Desk.
- 3.17. **Security Awareness Training:** Staff will be introduced to basic security principles and expectations as part of the New Employee Orientation Program. This training is conducted by IT using the "New Employee IT Orientation" document, as amended from time-to-time. Each staff member must be knowledgeable of basic security issues and their importance. Security awareness training is an ongoing process as hardware and software systems, and threats to those systems, change. Refresher training will be conducted on at least an annual basis to cover the following items: 1) Changes in the Security Policy since the previous refresher training, 2) Current security items that need strengthening based on known information or incidents, and 3) Items that have been noted in any audit findings.
- 3.18. **ITSP Document:** Additional specific information describing current policies and procedures is available on the IT Intranet web site and in the "City of Scottsdale's Information Technology Security Policy" document. Staff directly responsible for the setup or administration of hardware or software systems, including the administration of application systems, must review the information contained within that policy document. The current version of the policy document is available on the IT Intranet web site.
- 3.19. **EXCEPTIONS:** The City of Scottsdale acknowledges that there may be exceptions to this AR. These exceptions will require a documented risk assessment by the IT Network Security Engineer. Risk management is the process of balancing the cost of protecting against a risk vs. the cost of exposure. The Network Security Engineer will approve all decisions regarding risk of a security breach vs. the cost of protecting the information and/or computer information systems, in consultation with the City Auditor's Office, City Attorney's Office, Risk Management and the Executive Director –IT/CIO.

4.0 PROCEDURES

- 4.1. **Network and System Access:** Initial access to the City of Scottsdale network and enterprise resources is granted after the hiring division submits the online "New Hire" request. Subsequent requests for changing or removing a staff account can also be found on the IT Intranet web site.
- 4.2. **Staff Training:** All staff must be briefed on their responsibilities for computer information systems security before initial access is given to any City of Scottsdale computing system. Staff must also be updated at least annually on their security responsibilities. To satisfy this requirement, the following items will be provided:

AR136 – NETWORK AND COMPUTER SECURITY

- New staff will be introduced to basic security principles and expectations as part of the new employee orientation program. This training is conducted by IT using the "New Employee IT Orientation" document.
- Staff must communicate to their supervisor or the IT Security Office when they become aware of a security violation or concern. Staff must be aware of indications of non-secure activity. These indications include the items listed below:
 - Missing or altered files, programs, or data.
 - Anyone in a non-public area not wearing a City ID badge.
 - Conduct by others, both inside and outside the organization, indicating non-secure actions.
- IT will provide an online training program that covers the basic aspects of security issues and staff responsibilities in adhering to existing policies. Urgent and timely security information will continue to be shared with staff through existing communication channels such as:
 - Email notices
 - Intranet / CityLink
 - Computer Based Training
- Security awareness training is an ongoing process as hardware and software systems, and threats to those systems, change. Refresher training will be conducted on at least an annual basis to cover the following items:
 - Changes in the Security Policy since the previous refresher training.
 - Current security items that need strengthening due to known incidents.
 - Items that have been noted in any audit findings.

4.3. **Specialized Training:** IT staff and other recognized technology professionals in the City of Scottsdale organization may require additional education and training related to proper security configuration of hardware and software products that the City operates or is evaluating for use. IT and other divisional management should plan for such specialized training.

5.0 RESPONSIBILITIES

5.1. **Individual Staff Member Responsibility:** Staff members are responsible for following the policies described in Section 3.0 of this AR. Staff must communicate to their supervisor or the IT Security Office when they become aware of security issues or concerns.

Any deviations from the established security requirements are considered practices potentially dangerous to the overall security of the City's computing infrastructure and resources. Such deviations may result in compromise of information, inadvertent disclosure of sensitive information, unnecessary exposure or endangering City of Scottsdale assets, or actual loss.

AR136 – NETWORK AND COMPUTER SECURITY

- 5.2. **Reporting Security Violations:** All suspected information security incidents must be reported IMMEDIATELY to the employee's immediate supervisor. If that individual is unavailable, the next contact must be either the IT Network Security Engineer or another member of the IT Management Team. The IT Network Security Engineer will maintain a record of these incidents. All suspected security violations will be investigated by IT to establish responsibility for the violation and to estimate the possible consequences to the City's computing resources.
- 5.3. **Coordination between IT and HRS:** Human Resource Systems will notify IT regarding personnel changes (i.e. new hires, transfers, and terminations). Involuntary terminations must be reported to IT concurrent with the termination.

Human Resource Systems will work with IT to investigate any reported incidents of non-compliance with this AR.

6.0 OVERSIGHT/REVIEW

- 6.1. This AR outlines policies that staff must follow to help ensure the security of our computer information systems and networks. The IT Division also implements a number of process controls to protect these assets against loss or misuse. The major controls that affect staff are:
- Initial passwords for new hires are kept confidential until Employee Orientation or job start. Upon starting, the network requires that a "strong" password be selected.
 - Web and electronic communication usage information is logged to identify potential non-business use.
 - Support Desk staff will require basic identity verification prior to resetting a user's password.
 - Non-technical staff does not have administrative privileges on network workstations.
 - Anti-virus signature files used to detect the latest virus threats are updated automatically.
 - Vendor security patches are updated automatically, wherever possible.
 - All network workstations may be periodically scanned for unauthorized software or files.
 - Additional security awareness training, plus a cable lock, is provided for laptop users.
 - Purchasing requires prior IT concurrence for all software and hardware purchases.
 - Phone system usage information is logged for management review.
 - Regular internal testing and analysis are used to help identify potential vulnerabilities.
 - Security awareness training for staff will be regularly reviewed and updated.

AR136 – NETWORK AND COMPUTER SECURITY

7.0 DEFINITIONS

- 7.1. **Authentication:** The process of verifying an identity claimed by or for a system entity.
- 7.2. **Authorization:** Authorization is the process of granting a right or permission to access a system resource. Usually, authorization is in the context of authentication; once a user's identity has been authenticated, that user is enabled to perform the different types of access or activity for which s/he is authorized.
- 7.3. **Password:** A password is a secret data value, usually a complex character string, which is presented as part of an authentication process to verify an identity. Passwords are the most common type of computer system authentication mechanism used today.
- 7.4. **IT Support Desk:** The Information Technology Helpdesk (ext. 27827) provides assistance, problem resolution, and work-order submission for computer, networking, and telephony problems.
- 7.5. **Security Policy:** A security policy is a set of rules and practices that regulate how a system provides security services to protect sensitive and critical resources.
- 7.6. **User:** A User is someone who uses a computer information system or network. For the context of the AR, "user" means either the employee or authorized staff member that is accessing a system.
- 7.7. **Virus:** A computer virus is any computer software program or script that causes or influences either hardware or software to operate in a manner contrary to the intentions or in a manner unapproved by the original owner/user of said software or hardware. Viruses may be intentionally or inadvertently introduced into a computer system or network and then spread or self-replicated to other systems. Examples of how viruses can be spread are the use of flash drives, or CD-ROMs acquired from external sources, opening unexpected e-mail attachments, or downloading files from non-business Internet sites.
- 7.8. **Workstation:** For the context of this AR, "workstation" means the same as personal computer (PC) or terminal. This may be either a desktop or laptop computer.

8.0 RELATIONSHIPS TO ADOPTED POLICIES AND ORDINANCES

- 8.1. Electronic Communications – AR127
- 8.2. Personal Electronic Communication Device Usage – AR128
- 8.3. Internet Use – AR165

9.0 LINKS TO SUPPORTING DOCUMENTS

- 9.1. Electronic Communications – AR127
- 9.2. Personal Electronic Communication Device Usage – AR128
- 9.3. Internet Use – AR165

AR136 – NETWORK AND COMPUTER SECURITY

10.0 REVIEWED/AMENDED DATE(S) AND NOTES ON SIGNIFICANT CHANGES:

- 10.1. Original Effective Date: 02/01/2003
- 10.2. Updated 08/01/2011 – Reviewed and updated entire document including migration to the newly adopted AR format.