




AR165 – INTERNET USE

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

1.0 **PURPOSE**

- 1.1. The City of Scottsdale provides, to authorized staff, limited access to resources available on the Internet for the purpose of conducting City business and to facilitate communications with other agencies and business partners.
- 1.2. This Administrative Regulation ("AR") specifies the policies and procedures that are to be reviewed and practiced by all staff requesting access to, and using the, Internet.

2.0 **APPLICABILITY**

- 2.1. The definition of "staff" for this AR includes all employees, contract staff, and volunteer staff. This service is available, subject to supervisory approval, to all City employees and other authorized staff. Divisions or departments may require additional justification, restrictions or approval levels, as needed.

Note: Currently, all staff in PD/USB, PD/USB, PD/ISB, Fire, and the City Attorney's Office have Internet access by default when the staff account is created and do not require further action.

3.0 **POLICY**

- 3.1. City resources used to access the Internet may only be used for lawful, work-related purposes by City staff. Staff should keep in mind that anything they access, post or send over the Internet will reflect upon the City's image because the City's domain name and Internet address are associated with each transmission. All use of the Internet is logged and subject to monitoring to ensure compliance with existing City policies. City equipment and resources are intended for City business use only. 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.
  - **Default (Limited Access:** By design, every authorized network user has access to a limited number of Internet sites. These include City run web sites, City affiliated medical providers, most government web sites, and City designated business partners (e.g. Municode.com, OfficeDepot.com, etc.). No request is needed for this level of access.
  - **Standard Internet Access:** Internet access for staff is initiated upon receipt of written supervisor authorization. All Internet access requests require submittal of

## AR165 – INTERNET USE

an IT "Internet" work order. Once approved, access will be granted within three (3) business days. The requestor will receive a confirmation notice upon completion of the work order. Standard Internet access enables staff to access the most common resources required to perform their job functions. Many non-business Internet sites are limited or blocked as part of the City's overall network security strategy. Any exceptions made in granting access to additional Internet resources will require written authorization from the requestor's supervisor, as well as concurrence from the Network Security Engineer.

### Examples of unacceptable uses of the Internet include:

1. Using City time and resources for personal gain.
  2. Using City time and Internet resources for non-job related reasons including, but not limited to, the following:
    - a. Visiting news, sports, auction, shopping, travel, music, financial, or other sites that are not specifically required by your job responsibilities.
    - b. Using the City's email system for personal use (i.e., sending or receiving personal email).
    - c. Accessing personal websites or personal email using City resources.
    - d. Accessing personal chat or "blog" websites not approved by your supervisor for work purposes.
  3. Engaging in activity that wastes technology resources including bandwidth, file space, printer output, or other technology related resources.
  4. Sending or posting City confidential materials outside of the City, or posting City confidential materials within the City to non-authorized personnel. This includes blanket forwarding of City email to personal or private email accounts.
  5. Any activity that is in conflict with existing City values and policies.
  6. No VPN or direct external connections to outside networks (including home networks) are allowed without prior business justification and approval of the IT Security Engineer.
  7. Email and other electronic transmissions that are sent or received using City electronic resources are considered to be the property of the City of Scottsdale and are subject to review by City staff. Each employee is reminded that when using the City's network and computing resources there is no individual right of privacy with regard to equipment usage, or communications generated or received.
- **Emergency Use:** On occasion, an emergency may arise where the employee needs to use the Internet for a non work-related purpose. In this situation, the employee will notify his/her supervisor in writing of the emergency at the time, or as soon afterwards as possible. This notification should include an explanation of the emergency and the Internet resources that were used.

## 4.0 PROCEDURES

- 4.1. **Staff:** Staff members requiring Internet access for their assigned job function will need to have his/her supervisor submit an Internet access request to the Information Technology Support Desk.

Staff is responsible for understanding and adhering to AR# 165.

## AR165 – INTERNET USE

Staff recognizes that all Internet activity is monitored and logged. Inappropriate use will be reported to Human Resources.

- 4.2. **Management:** When a staff member requests Internet access, it is the responsibility of the supervisor to ensure that the reason for the request is legitimate, and intended to benefit the organization. The supervisor will then need to contact the Information Technology Support Desk requesting Internet access for that staff member. Information Technology will keep a copy of the request on file.

Supervisors may request a report on Internet usage by their staff by first contacting their departmental HR representative.

- 4.3. **Information Technology Staff:** The Information Technology Support Desk personnel are responsible for creating the Internet access work order, attaching the written authorization and enabling Internet connectivity. If a request for Internet access is received directly from a City staff member, the IT Support Desk personnel will only process the request if an authorizing email is received from the staff member's supervisor. It is the responsibility of the IT Support Desk personnel to keep a copy of this documentation along with the initial request.

### 5.0 RESPONSIBILITIES

- 5.1. **Employee:** It is the responsibility of every employee to use the Internet responsibly and in the interest and furtherance of City business. Staff members are required to read and understand the policies and procedures regarding the use of the Internet prior to being allowed connectivity. These additional policies and procedures can be found in Sections 8 and 9 below.
- 5.2. **Management:** If a supervisor has reason to believe or, it has been reported to the supervisor by another staff member, that an employee under his/her direct supervision may have engaged in any prohibited behavior with or inappropriate use of the Internet, it is the manager's responsibility to contact the Human Resources Executive Director, or designee(s), who will guide the supervisor through the process of documenting the allegations.

### 6.0 OVERSIGHT/REVIEW

- 6.1. **Connectivity:** All workstations on the City's network are capable of having Internet access. Requests for Internet connectivity must be submitted to the Information Technology Support Desk (see Sec. 4, Procedures)
- 6.2. **Monitoring:** Use of the City's electronic resources is monitored by designated City staff to ensure adherence to this AR. Workstation anti-virus alerts are investigated to determine the cause, as well as the impact, of the incident. The IT Security Team will determine when and if a computer system should be removed from the network for virus remediation or possible re-imaging. Infected systems may be shut down by IT staff without prior notice in order to safeguard the City's network and/or other computing systems.
- 6.3. **Logging:** All Internet destinations are logged by the City's web and email filtering servers and firewall security systems. Authorized City staff reserve the right to interrupt activity that interferes with the performance of the City's computer

## AR165 – INTERNET USE

systems or networks, or that conflicts with authorized use of City resources or equipment. High volume and/or non-standard use of Internet resources are reviewed regularly. Concerns about possible usage violations of this AR are forwarded to Human Resources for review and follow-up.

### 7.0 DEFINITIONS

- 7.1. **City Staff:** Includes all City employees, contract staff and volunteer staff.
- 7.2. **Internet Use:** The use of any and all systems designed to support business access to the World Wide Web (WWW), electronic mail (Email), and other electronic services provided via the City's Internet connections.
- 7.3. **IT Support Desk:** This is the Information Technology Support Desk (ext 27827), which provides assistance, problem resolution, and work-order submission for computer networking, radio, and telephony problems.
- 7.4. **Electronic Resources:** All types of computer workstations, laptops, servers, networking equipment, radio equipment, telephones (cell phones, smartphones, pagers) and telephone systems, City applications and system software, the Internet and the Intranet.

### 8.0 RELATIONSHIPS TO ADOPTED POLICIES AND ORDINANCES

- 8.1. Electronic Communications – AR127
- 8.2. Personal Electronic Communication Device Usage – AR128
- 8.3. Network and Computer Security – AR136

### 9.0 LINKS TO SUPPORTING DOCUMENTS

- 9.1. Electronic Communications – AR127
- 9.2. Personal Electronic Communication Device Usage – AR128
- 9.3. Network and Computer Security – AR136

### 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.