CITY OF HOUSTON

Executive Order

Subject: **POLICY ON INFORMATION TECHNOLOGY SECURITY**	E.O. No. **1-48**
	Effective Date: **November 3, 2003**

1. PURPOSE

   1.1 To provide consistent policies regarding Information Technology (IT) Security and the roles and responsibilities of personnel using and maintaining computer resources, electronic communications and Internet access in the performance of their job function.

2. OBJECTIVES

   2.1 To maintain the availability, integrity and security of the City's computer systems, devices, and data while minimizing the City's risk of loss and liability.

3. DEFINITIONS

   3.1 Authorized Users - any city elected or appointed official, city employee, temporary city employee, contractor, consultant, or any other individual authorized to use, operate or maintain any city system or access any system information. The term shall not include an individual to the extent that such individual's use of any city system is limited to using city computers under any program or service provided by the city to the general public.

   3.2 System - any electronic data transmission, communication or information storage or retrieval equipment device, program or system, owned, leased or operated by the city, including, without limitation, personal computers or laptops, computer networks, computer terminals, personal data assistants, data storage media, or telephone and facsimile transmission systems and devices, and printers, monitors or information display devices.

   3.3 System Information - electronically transmitted or stored data, voice or video content or any information generated or accessible through any city system or component thereof.

4. SCOPE

   4.1 This executive order applies to all city systems, system information and authorized users. Each authorized user, including authorized third party users who access city systems, will be held accountable to this policy.

   4.2 This executive order outlines the responsibilities of authorized users in placing, utilizing or accessing information on city systems, authorizes monitoring of users' activity for abuse, and establishes acceptable guidelines for system operations and

security.

4.3 This executive order also establishes that city system information including any data, voice or video content that is created, stored, distributed, found or displayed on city owned networks, computer terminals, personal data assistants, storage media (disks, memory sticks, etc.), or any other system device, is the sole property of the City of Houston and is subject to city policies and applicable laws. This principle includes information associated with any personal use of city systems by authorized users. Authorized users are placed on notice that no such information is subject to any expectation of personal, proprietary, or privacy rights on the part of any authorized user.

5 RESPONSIBILITIES

5.1 The Information Technology Department ("ITD") is responsible for managing and supervising the City's information and communications' systems. The ITD shall have the responsibility of providing an available, reliable, and secure communications infrastructure and is authorized to establish necessary procedures to ensure operability and security for system use, optimizing systems and monitoring network performance, security, activity, and abuse. Subject to the applicable provisions for establishing Administrative Procedures, the ITD is authorized to draft and administer any Administrative Procedures necessary to implement this policy as set forth in this Executive Order. The ITD is authorized to monitor and disclose electronic communications only as necessary to (i) assist in investigations of abuse or misuse of the City's IT system or (ii) perform evaluations or assessments of the system's use or functionality. The ITD will keep the Technology Steering Committee involved and informed on security matters, will not abuse this authority, and will perform such activities in compliance with applicable law and solely for the purposes of ensuring optimal system security and performance or assisting an authorized investigation.

5.2 City department directors are responsible for ensuring that authorized users under their supervision understand and comply with this executive order and any procedures authorized hereunder, and that necessary action is taken to authorize access to equipment, ensure proper accountability of physical system assets, maintain appropriate records, and report security breaches or illegal activity.

5.3 Each authorized user granted system access must comply with ITD system policies and handle assets such as passwords, identification codes, city confidential information and physical system assets in a secure and responsible manner. Authorized users, through their use of city systems and handling of city data and information, will be subject to monitoring. Use of city systems and handling of city data constitutes consent to monitoring. Authorized users will be required to comply with appropriate computer security precautions and virus protection procedures, including restrictions on connecting or attaching non-city computer equipment or other devices to city systems or installing unauthorized software. Authorized users will also be required to participate in training programs relating to matters within the scope of this executive order and to keep abreast of such supplemental or updated procedures as may be implemented from time to time under authority of this order.

5.4 The ITD is responsible for maintaining an IT security plan and assessing the acceptable levels of vulnerability for city IT assets, based on the criticality of the assets, on a regular and routine basis as described below.

6 SECURITY POLICY

6.1 It is the policy of the City to provide for the security of information technology systems through a multi-layered approach that includes, without limitation, IT policies and procedures, user training programs, improving defenses against misuse of hardware and software and other city IT systems, and defining the roles and responsibilities of city departments and authorized users in protecting system assets from unauthorized use, damage or disruption.

6.2 Furthermore, it is the policy of the City to maintain an inventory of IT assets and, on a routine and regular basis, assess the criticality of each major asset, e.g., the 911 call system, the Police and Fire Dispatch System, the Accounting Systems, etc., as well as the vulnerability of to these assets to threats. The City's security plan will be amended from time to time to improve the assets' defenses as needed to thus mitigate the risks from threats.

7 USE POLICY

7.1 Authorized users will utilize system equipment and information only when and as authorized by appropriate city authority, and only in the fulfillment of their assigned duties or for limited, incidental personal use consistent with subsection 7.1.16 of this section. All persons working for, under the direction of, or on behalf of the City are specifically prohibited from any of the following actions:

7.1.1 Accessing city IT system resources without express authority and compliance with city policies;

7.1.2 Using City computer resources for any illegal activity or personal financial gain;

7.1.3 Conduct which fails to protect physical system resources (including, but not limited to desktop, laptop, PDA, radio, fax machine, phone, etc.) From theft, loss, damage or destruction;

7.1.4 Unauthorized disclosure of city passwords, codes or identification numbers;

7.1.5 Unauthorized disclosure of city data, voice or video content;

7.1.6 Knowingly disrupting city system resources;

7.1.7 Unauthorized alteration, damage or destruction of any city system resources, including content;

7.1.8 Authorizing the use of city system resources beyond delegated authority limits;

7.1.9 Unauthorized copying of proprietary software, media, or copyrighted material;

7.1.10 Data, interruption of computer services or other loss or harm;

7.1.11 Unauthorized interception, or assisting in the unauthorized interception or monitoring of electronic communications not intended for the employee;

7.1.12 Knowingly introducing a harmful program or set of instructions into a computer's memory, operating system or program including, but not limited to, a computer virus, which causes or could cause a partial or total alteration, damage or erasure of stored data, interruption of computer services or other loss or harm;

7.1.13 Knowingly causing the transmission of a program, information code or command to a city computer resource that will cause damage to a computer, computer system, network, information data or program or which will improperly withhold or deny the use of a computer, computer service, computer network, information, data or program or cause the unauthorized release of information or data;

7.1.14 Attempting to circumvent or defeat security or auditing systems of any city ITD system or application without prior authorization or permission;

7.1.15 Using internet access, electronic mail, voice mail or other city communications systems for purposes not related to city business, except as provided under section below, or for activities inappropriate or generally offensive in the workplace including, but not limited to:

7.1.15.1 Political or commercial usage;

7.1.15.2 Viewing, downloading or transmitting sexually-oriented or explicit material, data, or graphics;

7.1.15.3 Demeaning any person or group of persons on the basis of race, ethnicity, gender, disability, beliefs concerning religion, or sexual orientation; or

7.1.15.4 Any communication or usage violative of any rule or guideline governing employee conduct set forth by executive order, administrative procedure, departmental policy or ordinance.

7.1.16 Personal use of internet access, electronic mail, voice mail, or other city communications systems other than incidental use, limited in duration, that does not impact job performance or violate any of the foregoing prohibitions.

Any violation of the policies established under this executive order may result in disciplinary action, up to and including termination of employment, and may also result in prosecution under the provision of any applicable law. Violation of these policies by any person other than an employee or official of the City of Houston may result in termination of contract(s) or service agreement(s) and/or prosecution under the provision of any applicable law.