CITY OF SACRAMENTO

ADMINISTRATIVE POLICY INSTRUCTIONS

Topic: Information Technology Resource Policy

Effective Date: 5/10/2004

From: Information Technology Department

Supersedes: 5/20/2002

To: Department Directors/Division Managers
Information Technology Resource Users

Section: API # 30

TERRY LEUCHARS
Interim Chief Information Officer

APPROVED:

ROBERT P. THOMAS
City Manager

SUMMARY OF CONTENTS

1. PURPOSE

1.1. The purpose of this Administrative Policy Instruction (API) is to establish a policy and guidelines for the acceptable use and security of the City's Information Technology resources.

The City of Sacramento relies on its Information Technology Resources to conduct official business. The City has created this Information Technology Resource Policy to ensure that Information Technology Resources are used properly by its employees, contractors, agents, and other resource users.

The rules and obligations described in this policy apply to all "Users" of the City's Information Technology Resources, wherever they may be located. Violations may result in disciplinary actions, up to and including termination, and civil and/or criminal liability.

It is every user's (as defined by section 3.2) duty to use the City's Information Technology Resources responsibly, professionally, ethically and lawfully.

2. SCOPE

2.1. This API sets forth policies and standards for the acceptable use and security of the City of Sacramento ("the City") Information Technology resources.

2.2. This API applies to all users of Information Technology resources in the City unless an "exception" request is submitted in writing to, and approved by, the Chief Information Officer ("the CIO"), or his or her designee.

3. DEFINITIONS

3.1. Information Technology Resource

Information Technology Resources are tools that allow access to technological devices, or are technological devices themselves that service information, access information, and the information itself. These resources include all City-provided computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; peripheral devices such as printers, scanners and cameras; pagers, radios, voice messaging, facsimile transmissions, copy machines, electronic communications, external network access such as the Internet; software, including packaged and internally developed applications; and all information and data stored on City equipment as well as any other equipment or communications that are considered an Information Technology Resource.

3.2. User of an Information Technology Resource

The User is defined as any person who uses Information Technology Resource. This includes employees, contractors, consultants, vendors, volunteers, temporary agency employees, guests, student interns and any other person who may have access to Information Technology resources.

4. POLICY ENFORCEMENT

4.1. The Chief Information Officer (CIO) and his or her designee shall have the primary responsibility for enforcing this API. The CIO will be responsible for the establishment of policies, operating procedures and guidelines governing the technical architecture, usage, security, backup and recovery for Information Technology Resource.

4.2. Any user who violates this API may be subject to discipline, up to and including employment or contract termination, civil and criminal liability and removal from City premises.

4.3. Any user learning of or reasonably suspecting any misuse of Information Technology Resource shall notify his or her supervisor, who shall notify the CIO or his or her designee.

4.4. Any user who receives communication or messaging that he or she reasonably suspects may be illegal or may reasonably be considered offensive, disruptive, harassing, defamatory or threatening towards the City, any user, or any third party shall advise his or her supervisor, who shall notify the CIO or his or her designee.

4.5. The absence of written policies, procedures, standards, or guidelines governing a specific issue does not relieve the user from the responsibility for the acceptable use and security of City provided Information Technology Resources.

4.6. Authorization for access to Information Technology Resource must comply with criteria, reviewed and approved by the CIO or his or her designees.

4.7. All Information Technology Resource users must complete and submit a "User Acknowledgement Form" (Exhibit A in this API). Existing employees shall complete and submit the form within 30 days of implementation. New users shall complete and submit the form before access is granted to Information Technology Resources.

5. ACCEPTABLE USE

5.1. The City is the sole owner and may monitor and disclose contents and usage at any time of any Information Technology Resource provided to users. There is no reasonable expectation of privacy in the use of any Information Technology Resource.

5.2. Users are responsible for the acceptable use and security of Information Technology Resource designated for their use even if another group, division, or agency has been subcontracted to provide the support for these resources. Furthermore, if Information Technology Resources are sold or released while in the possession of a user, the user may be subject to discipline, up to and including employment or contract termination, civil, criminal liability, and removal from City premises.

5.3. Information Technology Resources shall be used for official City business. Information Technology Resources may also be used for incidental personal use, so long as such use does not result in a significant monetary expenditure to the City or involve the expenditure of a significant amount of time by the user away from his or her job duties. Supervisory personnel are responsible for limiting personal use of Information Technology Resource.

5.4. Abuse of this policy may subject the user to discipline, up to and including employment or contract termination and removal from City premises. In determining whether to impose discipline, the following factors will be taken into account: (1) whether the use interferes with the

user's or any other user's job duties or routine business activities; (2) whether the use results in significant expense to the City; (3) whether the use is for illegal practices, personal financial profit, outside employment, or user's promotional activities; or, (4) whether the use compromises any other City policies.

5.5. Information Technology Resources must not be used for or contain any material that may reasonably be considered offensive, disruptive, harassing, defamatory or threatening towards the City, any user, or any third party. Furthermore, users are prohibited from engaging in any internal or external communications using Information Technology Resources that refer to violence, racism, sexism, drugs, illegal conduct, pornography, gambling, betting, or other subjects that would be offensive to a reasonable adult in the work environment. Nothing in this section shall be construed to preclude any use that is objectively reasonably necessary for the performance of an employee's job responsibilities.

5.6. Any Information Technology Resources assigned to or in the possession of a user must be returned to the City when City management determines that the use of those resources is no longer required to conduct official City business.

5.7. Information Technology Resources that are for the purpose of external contact by the general public shall be reviewed and approved in writing by management of the department or organization submitting the information for public access.

6. GENERAL SECURITY

6.1. Information Technology Resource users are responsible for the protection and security of Information Technology Resources. Information Technology Resources shall be protected, to the extent reasonably possible, from misuse, including, but not limited to: theft, unauthorized access and data transfers, fraudulent manipulation or alteration of data, attempts to circumvent the security controls, and any activity that could compromise the integrity or availability of data.

6.2. Users shall not violate software license agreements or any other contractual terms and conditions of using Information Technology Resources regardless of whether harm is intended.

6.3. Users are prohibited from introducing any unauthorized Information Technology Resources into the City's environment or infrastructure. Furthermore, the introduction of any Information Technology Resources that could disrupt any operations is prohibited.

6.4. Information Technology Resources must be free of viral infections. Virus detection devices and tools must be installed and kept up-to-date on appropriate Information Technology Resources. Furthermore, any external Information Technology Resources introduced into the environment must be scanned or reviewed for any threats before being entered into the environment.

6.5. Written Information Technology Resource Policies will be issued and updated on an as-needed basis, in conjunction with this API. New or revised Policies will be published to all users via GroupWise email and made available to all users on the City's intranet site (http://www.mysacramento.org/security). It is the responsibility of users to check this intranet site when the user receives notification of modifications to the Guidelines.

6.6. Users are prohibited from violating any established written policies or guidelines that are designed to control or enforce this Information Technology Resource policy.

7. EXHIBIT A - USER ACKNOWLEDGEMENT

A signed paper copy of this form must be submitted, as indicated in section 4.7 of the Information Technology Resource Policy, for authorization of a new user-ID and/or access to any Information Technology (IT) resources. An electronic acknowledgement must be completed for authorization of a change in privileges associated with an existing user-ID, or periodic reauthorization of an existing user-ID. The City will not accept modification to the terms and conditions of this agreement.

User Name (Printed): _____

User's Department: _____Org#_____

User's Business Telephone Number: _____

User's Business Address: _____

I, the user, agree to take all reasonable precautions to assure the City's internal information, or information that has been entrusted to the City by third parties (such as customers), will not be disclosed to unauthorized persons unless required by law. At the end of my employment, appointment, or contract, with the City, I agree to return to the City all Information Technology Resources to which I have had access in order to do my job. I understand that I am not authorized to use any Information Technology Resource for non-employment related purposes, nor am I at liberty to provide any Information Technology Resource to third parties without the express written consent of the City Manager and/or designee.

I have access to a copy of the City's Information Technology Resource Policy (API #30). I have read and understand this policy and its relationship to my job. I understand and agree that violation of the City's Information Technology Resource Policy (API #30) may be grounds for discipline up to and including termination of my employment, and I agree to abide by the Policy as a condition of my employment. I understand that written Information Technology Resource Policies will be established for Information Technology Resources, in conjunction with this policy, and that the written policies will be made available by the Information Technology Department on the City's Intranet web site. Information Technology Resource policies will be updated and communicated to all users of the resource I understand and agree that it is my responsibility to read the policies and all updates as they become available, and I agree to be bound by and adhere to those policies. Printed copies of the current policies are available through the City's Information Security Office I understand that non-compliance may be cause for system privilege revocation, disciplinary action up to and including termination, as well as criminal or civil penalties.

I also agree to promptly report all violations or suspected violations of Information Technology Resource Policies and Guidelines to my supervisor, who shall notify the CIO or his or her designee.

User Signature & Date: _____

8. EXHIBIT B - IT RESOURCE CHANGE CONTROL POLICY

Purpose

The purpose of this Information Technology Resource Change Control Policy is twofold:

- To protect the City's technical infrastructure by governing a citywide Information Technology (IT) change management process that minimizes the risk and impact of changes to the City's networks, servers, mainframe systems and business applications; and
- To coordinate and inform citywide users of all changes that impact the City network systems and/or services.

The intent of this policy **is not** to question the rationale of a change, but to insure that all change elements are in place, all related parties are notified and trained, and the schedule for implementation is coordinated with all other activities on the City's network and production environment. This Policy governs the ongoing process of communicating, coordinating, monitoring and scheduling changes to the City's Information Technology environment. This Policy supports, provides clarity to, and is implicitly sanctioned by API # 30 (City Information Resource Policy).

Scope

This Policy applies to any activities that make different, alter, modify, or impact the City's networks, servers, mainframe systems and/or business applications. These activities will be referred to as "IT Changes" and include all hardware, systems software, application software, or procedural changes that could impact the City's network and production systems and/or the City's IT services. This Policy sets forth the rules and requirements for all IT Changes. The rules and requirements described in this Policy apply to all City's employees, contractors, and/or agents doing business with the City. Violations will be taken very seriously, and may result in disciplinary actions as sanctioned in API #30.

An IT Change Control Process has been developed and will be updated on an as-needed basis, in conjunction with this Policy. The IT Change Control Process describes the steps, forms, meetings and detailed actions necessary to comply with the rules and requirements of this Policy and to obtain approval for implementation of IT Changes to the City's IT infrastructure. The IT Change Control Process is published and made available to all users on the City's intranet site. It is the responsibility of all users to check this intranet site periodically to ensure that they maintain continuing compliance with this policy and its related IT Change Control Process. The Process has the following objectives:

- To allow changes, while at the same time maintaining or improving service stability and availability.
- To reduce or eliminate reworks and/or changes that may need to be backed out, due to inadequate preparation.
- To ensure that all parties affected are informed of planned and authorized changes.
- To provide a record of IT Changes implemented to assist with and shorten future problem determination and/or troubleshooting time.
- To ensure technical and management accountability for all IT Changes is identified.
- To assist with the accuracy of predictions of impact, such as response time and utilization.
- To ensure that all affected parties are not only informed, but also necessary documentation and training, if required, is in place prior to the implementation.

Overview of IT Change Control Process

All proposed IT Changes are to be reviewed and approved by the IT Change Control Committee prior to implementation. The IT Change Control Committee will consist of representatives from each function/discipline in the IT department as outlined in the IT Change Control Process. The IT Change Control Committee will perform the function of providing Quality Assurance for each requested IT Change. In this capacity the IT Change Control Committee has the responsibility to ensure that appropriate documentation, testing, notification, training (of both users and support staff, if required), and back out/recovery procedures are in place for each IT Change requested. The IT Change Control Committee will authorize, coordinate, track, evaluate, and verify changes to the City's network and systems. The IT Change Control Committee will:

- Establish and oversee the IT Change Control Process for the City.
- Meet as frequently as needed to review the IT Changes requested and to authorize, reject or defer the requests made during the period.
- Select a coordinator from within its membership to be responsible for routing changes required to members of the City of Sacramento's Network Administrators (COFS) group. In addition, the coordinator will be responsible for summarizing and communicating all IT Changes made to the IT Change Control Committee.
- Refer to the Chief Information Officer any request(s), that in the collective judgment of the Committee, may have a significant impact on the City's network and/or mission critical systems/applications.
- Refer issues of non-compliance of the IT Change Control Process to the CIO for enforcement, corrective or disciplinary actions.

The Chief Information Officer (CIO) and/or his/her designee(s) shall have the primary responsibility for enforcing the Policy. Users are prohibited from violating any established written policies or guidelines that are designed to control or enforce this Policy. Any user who violates this Policy may be subject to discipline.