Remote Access 1.7.3

PURPOSE

The purpose of this policy is to provide guidelines for the use of remote access technologies, thereby extending the availability of the City's computing network, systems, data and applications.

The City provides remote access to the City network and systems to facilitate use of City applications and City data. Since these remote access methods provide external connections to the City network, it is critical to ensure that access is strictly limited to authorized users with business needs in order to ensure the security of the City networks, systems and data.

SCOPE

This policy applies to all City of San Jose employees, contractors and consultants requesting remote access to the City network. ***Remote access*** is defined as the connection to the City and network of any computer equipment that is not part of the Information Technology Department defined City Computer Network [Wide Area Network (WAN) and Local Area Network (LAN)].

POLICY

It is the administrative policy of the City that all remote access to the City's computing network shall be managed by the Information Technology Department. All requests for and uses of remote access shall conform to the stated procedures for authorization and implementation to ensure:

- The ongoing security of the City's computing and data resources.
- The appropriate use of the City's remote access resources.
- That the City's network, application and data resources are used for official City purposes only (e.g., use of the City network for personal Internet access or processing of personal e-mail is not appropriate).
- That authorization is limited to users with a well-defined business need.

Use of remote access to the City's computing network shall be used in accordance with the following provisions:

1. Any work done on the City's network using either City-owned or personal computing equipment is subject to all provisions of all applicable City Policies including City Policy Manual (CPM) Section 1.7.1, the "Use of Email, Internet Services & Other Electronic Media" and CPM Section 1.6.2, "Personal Use of City Equipment".

2. Due to the nature of remote access and its susceptibility to failures outside the City's control, remote access should not be used as access for ongoing mission critical applications.
3. All remote access connections will be automatically terminated after thirty (30) minutes of inactivity.

4. Non-exempt employees (non-salaried employees that are paid on an hourly basis and are non-exempt under applicable laws) must be compensated while performing authorized work remotely. Therefore, **any work performed by a non-exempt hourly employee by remote access needs to be approved in writing by his/her supervisor in advance of the work being performed.**

RESPONSIBILITIES

A. Requesting Department:

1. Individual requesting remote access completes the *Remote Access Authorization Form*.

2. Requestor's supervisor reviews the request, and if the request is appropriate forwards the form for signature by the requesting Department's Director.

3. Provides the requestor with the City's "Use of Email, Internet Services and Other Electronic Media" policy contained in City Policy Manual Section 1.7.1.

4. Departments are required to monitor Remote Access use for hourly employees to ensure that hourly employees are compensated for time worked and that such time is being approved in advance.

B. Information Technology Department:

1. Reviews request to ensure that all required information has been included and that the request has been appropriately authorized.

2. Establishes remote access account and supplies requestor with access information.

3. Evaluates, on a quarterly basis, account activity for relevancy and conformance to security policies and procedures.

4. Notifies remote access users and departments of any changes to specific accounts.

5. **Employees will not have Remote Access capabilities until the Information Technology Department has received and processed the completed and signed *Remote Access Authorization Form.***

C. End user responsibilities:

1. **Hourly (non-salaried) employees must have pre-authorization for any work done from a remote location.**

2. Any and all client software/hardware installation(s)

3. Ensure anti-virus is up to date prior to each connection to the City network.

4. Costs associated with the connectivity from the personal computer to the City network.

5. Maintain confidentially of the remote access usernames and passwords, including but not limited to:
   a. Not sharing usernames and passwords with others.
   b. Not writing usernames and passwords down.
   c. Not passing usernames and passwords via email.

PROCEDURES

The following procedure applies to all requests for remote access to the City's computing network:

Responsibility	**Action**
Employee/Contractor	1. Completes the attached *Remote Access Authorization Form*. Signs the form and submits form to department supervisor.
Supervisor and Department Director	2. Supervisor reviews request, and if approved, forwards to requesting Department Director. Director approves or denies request based upon department analysis of need for remote access. If request is not approved, notifies the requestor.
Department	3. If approved, requesting Department Director signs request form and forwards to the Director of Information Technology
Information Technology	4. Establishes an account on the remote access server, creates a password, and provides requestor and/or departmental network coordinator with information required to connect to the network.
	5. Evaluates account activity, on a quarterly basis, for relevancy and conformance to City policies and security procedures.
	6. Responds to requests for service relating to remote access system availability. Notifies affected account user, and associated department, of any account modifications.

Approved:

/s/ Kay Winter
Deputy City Manager

3/27/2006
Date

REMOTE ACCESS AUTHORIZATION FORM

☐City Employee ☐Contractor ☐Consultant

A. EMPLOYEE INFORMATION

Employee Last Name: | Employee First Name: | Employee ID#

Department: | Division: | Job Title:

Internet Provider: | Computer Location (address):

Connecting Phone Number: | Type of Access: Dial-Up ☐ DSL ☐ Cable ☐

Workstation Ownership: City Owned ☐ Personal ☐ | User Type: Telecommuter ☐ Remote Office ☐

B. DEPARTMENT AUTHORIZATION

Authorized Remote Access: Email ☐ City Network ☐ Employee Type: Non-Exempt (Hourly) ☐ Exempt (Salaried) ☐

By signing below I acknowledge that this request is consistent with the Remote Access Policy. If this request is for a non-exempt hourly employee (non-salaried employees that are paid on an hourly basis and are non-exempt under applicable laws), I understand that non-exempt hourly employees need to be paid for time worked using remote access and that this has been considered in making this request.

____ ____

Supervisor (print name & sign) Date Department Director or designee (print name & sign) Date

C. EMPLOYEE ACKNOWLEDGEMENT

1. **The password assigned to you must be protected at the same level as the information processed on the system(s). You are responsible for any activity on your account. *Initial*_________**

2. **Your password will be issued only once and will be immediately retired when the time limit has expired. Your password is unique to your user-id and identifies your individual system authority and privilege. It must not be shared with anyone else, even individuals working on the same project. *Initial*_________**

3. **Passwords shall not be included in script files for logon procedures, automatically programmed into function keys or written down. *Initial*_________**

4. **Anti-Virus Software must be up to date prior to each connection to the City's network. *Initial*________**

5. **If you believe that the confidentiality of you password has been compromised, contact IT Network Operations immediately. If your password is changed for any reason, you will be notified immediately. *Initial*_________**

6. **Any equipment connected to the City Network may be scanned and activity monitored to ensure the security of the City Network and Systems. *Initial*_________**

7. **Non-exempt employees must receive department authorization prior to using remote access. *Initial*__________**

I, the undersigned, acknowledge that I have read, understand, and accept all City of San Jose policies applicable to this request including City Policy Manual Sections 1.7.1 (Use of E-mail, Internet Services, and Other Electronic Media) and 1.7.3 (Remote Access Policy). I understand that if I am a non-exempt hourly employee I must obtain pre-approval of all work performed using Remote Access. I further understand that failure to comply with the applicable policies and rules related to remote access may lead to disciplinary action.

____

Employee Signature Date

D. SYSTEM INFORMATION

Host System Name:__________________________________ User Domain Name:____________________________________

Operating System (Name & Version): ________________________________ Existing Software Inventory:____________________

Anti-Virus (Name & Version)________________ Anti-Virus Definition Date: _____________ Anti-Virus Forced Update: Y N

System Configured By: _______________________________ Date:_______________ Extension:_____________

E. IMPLEMENTATION (ITD USE ONLY)

Network Operations Manager Authorization: _______________________________________ Date:_________________

Engineer Assigned: ___________________________ Date: _______________ Account Name: _____________________

Account Enabled: Y N Date: _______________ Remote User Notified on: ______________

Date

____ _____________

Chief Information Officer Signature Date