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 City systems. Remote access is defined as the connection to the City infrastructure from any computer equipment over the Internet including but not limited to Cloud based tenancy of 0365.

 POLICY

It is the administrative policy of the City that all remote access to the City's infrastructure 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 email 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 long-term, ongoing mission critical applications.

3. 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 by his/her supervisor. Approval should be obtained in advance of the work being performed absent extenuating circumstances.
RESPONSIBILITIES

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

B. End User Responsibilities
   1. All employees requesting remote access (for self or other person) should apply for remote access through the Request Remote Access Form available on the SimpliGov platform.
   2. All employees must read the instructions in the form carefully before filling in the items in the form.
   3. All employees must read the Information and Systems Security Policy and Expectations of Remote Access and acknowledge them.
   4. Hourly (non-salaried) employees must have pre-authorization for any work done from a remote location.
   5. Users connecting with personal devices, must complete installation of any and all client software/hardware installation(s).
   6. Ensure anti-virus is up to date prior to each connection to the City network.
   7. The users will bear any costs associated with the connectivity from the personal computer to the City network.

C. Department Supervisor
   1. Supervisors must determine whether employees need remote access to City resources to conduct business.
   2. Supervisors must review all the items in the request form and validate the need for access.
3. Supervisors can recommend approval or denial of the request and provide relevant comments in case of denial.

D. **Department Director**

1. The Department Director, or designee, must review all the items in the request form thoroughly and validate the need for access.

2. The Department Director, or designee, can approve or deny the request and provide relevant comments in case of denial.

3. 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.

E. **Chief Information Security Officer (CISO)**

1. The CISO must review the Request Remote Access Form.

2. The CISO relies on Director or designee approval of the need to conduct business remotely by the end user.

3. The CISO can approve or deny the request and provide relevant comments in case of denial.

**DEFINITIONS**

1. **Remote access** – Connection to the City infrastructure from any computer equipment over the Internet including but not limited to Cloud based tenancy of 0365.

2. **City systems** – Collection of computing devices and services owned, managed, and/or operated by the City.

3. **City computer network** – Communications infrastructure owned, managed, and/or operated by the City.

4. **City resources** – Any processing or storage technology owned, managed, and/or operated by the City.
## PROCEDURES

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

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee/Contractor</td>
<td>1. Completes the <a href="#">Request Remote Access Form</a> that is available on City’s intranet, fill the form, acknowledge, signs the form and submits.</td>
</tr>
<tr>
<td>Department Supervisor</td>
<td>2. Supervisor reviews request. If approved, forwards the request to Department Director, or designee, and must provide relevant comments in case of denial of request.</td>
</tr>
<tr>
<td>Department Director or Designee</td>
<td>3. Department Director or designee reviews request. If approved, forwards the request to CISO and must provide relevant comments in case of denial of request.</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>4. CISO reviews request. The CISO can approve or deny the request and provide relevant comments in case of denial of request.</td>
</tr>
<tr>
<td>Information Technology Department</td>
<td>5. 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.</td>
</tr>
<tr>
<td></td>
<td>6. Evaluates account activity, on a quarterly basis, for relevance and conformance to City policies and security procedures.</td>
</tr>
<tr>
<td></td>
<td>7. Responds to requests for service relating to remote access system availability. Notifies affected account user, and associated department, of any account modifications.</td>
</tr>
</tbody>
</table>

Approved:

/s/ Rob Lloyd \\
Information Technology Department Director \\
10/20/2020 \\
Date

Approved for posting:

/s/ Jennifer Maguire \\
Assistant City Manager \\
10/20/2020 \\
Date