CITY OF MILPITAS

Revision	Date
Original	11/23/2020

CITY ADMINISTRATIVE POLICY

Policy No: 2.6.1	**REMOTE ACCESS POLICY**	**Effective Date:** 11/23/2020
Revision No: Click or tap here to enter text.	**Policy Administrator:** Information Technology	**Next Review Due:** 11/23/2021
Related Policies and Procedures: N/A	**Approved by:** Steve McHarris, City Manager	**Date Approved:** 11/23/2020

1. PURPOSE

This Remote Access Policy lays out the requirements for designing and operating remote access solutions that aim to be more secure, controlled, auditable, and user-friendly.

The goal is to extend availability of internal network computer systems to outside locations while managing the inherent increased risks and vulnerabilities to an acceptable level.

The purpose of this policy is to define standards for connecting to the City's internal network and its interconnected information technology resources from any remote host device or system.

As individually determined, some or all provisions may also extend to cloud-hosted City technology resources.

Defined standards include baseline security requirements for users who remotely access the City network, permitted forms of remote access, and requirements for employees and third parties to gain access.

- ***Remote Access is provided as a tool to enable increased productivity of the organization.***
- ***Remote Access must not unduly expose computer systems, communication networks, and all processed and stored data to unacceptably increased risks.***

This policy is intended to minimize the potential exposure of the City's information resources to loss and damages that may result from unauthorized use. The use of secure authentication methods, meaningful authorization levels, and sufficiently detailed accounting and auditing tools is therefore central to all intentions of this policy.

2. POLICY

2.1. Except for those individuals who act exclusively in the role of an external end user of City-provided information technology systems (i.e. residents and customers), this policy applies to all Remote Access Users defined in section 3.2. of this policy.

2.2. All Remote Access is to be administered according to procedures stipulated in section 4. of this policy.

3. DEFINITIONS

3.1. **Trust Levels:** Successful authentication permits a user Remote Access at a specific authorization level, which depends on trust levels and approved demonstrated needs:

a) **Trusted users** include those in sections 3.2.G. through 3.2.J. of this policy, whose Remote Access request was approved.
b) **Untrusted users** include those in section 3.2.K. through 3.2.L. of this policy, whose Remote Access request was approved.
c) **Trusted devices** are City-issued Remote Access computers that are centrally managed domain members with centrally enforced operating system, application software, anti-malware software, and policy updates.
d) **Untrusted devices** are all those that do not comply with section 5.c)

3.2. A **Remote Access User** is anyone who:

a) Remotely accesses the City's internal network
b) Remotely accesses cloud-hosted City technology resources

Specifically, this includes:

A. All employees (full-time and part-time)
B. All staff contractors (third parties working in employee positions)
C. All elected officials (City Council members)
D. All appointed officials (Commissioners)
E. All interns and volunteers (paid or not)
F. All other individuals seeking remote access (vendors, contractors, etc.)

3.3. **Remote Access Technologies** include, but are not limited to, the following:

- Virtual Private Networks (VPN)
- Desktop-sharing systems (VNC, RDP, GoToMyPC, TeamViewer, etc.)
- Application virtualization (XenApp, App-V, etc.)
- Virtual terminal connectivity (Telnet, Secure Shell, etc.)
- Firewall access rules and exceptions
- Wired and wireless media, which can be either user-owned (home WiFi, etc.) or carrier-provided (mobile telecom devices, etc.)

4. PROCEDURE

4.1. **Remote Access Request and Approval**

All forms of Remote Access shall require a prior authorization request and approval procedure as outlined below:

a) Potential remote users must review the City's Remote Access Agreement and submit their request for Remote Access in written form to their Department head or designee by using a published IT Helpdesk online form.

b) Requests for Remote Access must be reviewed and approved by department heads or their designees. A list of all authorized designees will be maintained by the Information Technology department. Department heads shall review and confirm their list of authorized designees at the start of each fiscal year or designees will be removed from the authorization list within 30 days.

c) Department heads or their designees then forward the request along with their approval note to the IT Helpdesk.

d) Information Technology staff will implement authorized levels of remote access as approved.

e) Information Technology staff will provide department heads or their designees with lists of currently authorized Remote Access users at the beginning of each fiscal year. Authorization must be reconfirmed within 30 days or Remote Access authorization will be revoked.

4.2. **Remote Access Authentication**

All users of Remote Access shall require authentication as follows:

a) Users must be individually authenticated; shared or generic user accounts will not be authorized for any form of Remote Access.

b) Anonymous forms of Remote Access are not permitted at any time.

c) Some authorization levels may require multi-factor authentication with user credentials and additional device certification.

Remote Access authentication mechanisms are subject to the same user account and password polices as may be in force on the City's internal network.

4.3. **Remote Access Authorization Levels**

Appropriate Remote Access authorization levels shall be designed, implemented, and enforced by Information Technology department staff according to the following three trust level combinations of users and devices:

A. **Trusted users with trusted devices:** Authenticated Remote Access users will generally be authorized for most-privilege Remote Access, which extends most or all their usual work environment to their Remote Access computer.

B. **Trusted users with untrusted devices:** Authenticated Remote Access users will generally be authorized for privileged Remote Access, which extends most of their usual work environment to their Remote Access computer but may impose certain restrictions.

C. **Untrusted users** (regardless of device classification): Authenticated Remote Access users will generally be authorized for least-privilege Remote Access, which strictly limits authorizations to demonstrated and specifically approved needs only.

All those Remote Access users with untrusted devices are responsible for maintaining all available security features including, but not limited to, ensuring valid and up to date anti-virus and anti-malware software protection, maintaining current operating system and application security patches and hotfixes, etc.

4.4. **Accounting and Auditing**

Remote Access users agree to and accept that access and connections to City networks may be monitored to record dates, times, duration of access, activities, etc., in order to identify unusual usage patterns or other suspicious activity. As with all other in-house City computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

Audit information may be made available to department heads, Human Resources, and City Manager's Office upon request.

4.5. **General Remote Access Rules**

a) This Remote Access Policy shall be interpreted in addition to any other policies that may be in force and are applicable to the Remote Access user and/or the Remote Access device at any time. This policy is not intended to replace or modify any other policies that may exist elsewhere.

b) Direct Remote Access using any desktop-sharing system is not permitted; establishing a successful VPN connection prior to desktop-sharing is mandatory.

c) Direct Remote Access using any virtual terminal connectivity is not permitted except by authorized Information Technology department staff for emergency system administration purposes. Non-emergency use requires establishing a successful VPN connection prior to virtual terminal connectivity.

d) It is paramount that all Remote Access users follow applicable policies and procedures when accessing, processing, and storing confidential and/or restricted data, which is any data governed under Federal or State regulatory or industry compliance requirements such as HIPAA, FERPA, GDPR, GLBA, PCI/DSS, DCL3, Red Flag, and FISMA. This also extends to unclassified data deemed critical to the City's business processes which, if compromised, may cause substantial harm and/or financial loss.

e) Public Safety users of Remote Access must always bear in mind their additional compliance obligations, especially under the U.S. DOJ FBI's Criminal Justice Information Services (CJIS) Security Policy and related State and Local policies and regulations. For example, Remote Access might enable Public Safety users to intentionally or inadvertently circumvent internally implemented security measures that otherwise rely on the CJIS Security Policy's "Physically Secure Location" concept.

f) Any form of "Trojan Horse" tools to enable Remote Access in potential circumvention of external-inbound firewall access rule policies is prohibited. These include tools that are installed on internal host systems and quasi-permanently establish connectivity from the inside to an outside third-party proxy host system, thus enabling Remote Access to an internal host system through an established connectivity path without requiring an additional external-inbound firewall authorization.

4.6. **Remote Access Policy Violations**

Any irregularities of Remote Access use or violations of this policy may be subject to an administrative review by the City.

Violations of this policy may be cause for a range of disciplinary actions, up to and including termination of employment and/or criminal prosecution.