



## Remote Access Policy

**Purpose:** To establish policy regarding the acceptable use of the City and County of Denver's ("City") remote access systems by authorized users.

**Scope:** This policy is applicable to all City employees and other individuals authorized to use the City's remote access system ("User"). Remote access provides a means of connecting to the City's internal network by using remote access devices including all types of modems and routers such as analog modems, DSL devices, cable modems, wireless modems, telephones, handheld devices, etc. The policy defined below will address both the use and administration of remote access ensuring secure and appropriate use of the city's networks. The remote access system, hardware, software, tools and information are provided for the purpose of conducting business on behalf of the City only.

**Policy:** Remote access authorization must be acquired for all external connections to the City's internal network resources. In order to obtain authorization the remote user agreement must be signed and submitted.

Allowable use of the network and information via remote access include the following, to the extent that these uses are for the purpose of conducting City business:

- To facilitate performance of job functions
- To conduct research in accordance with an employee's job duties and functions
- To communicate with outside organizations as required to perform an employee's job functions.

Prohibited uses of the remote access systems and networked information include, but are not limited to, the following:

- Illegal activities
- Threats
- Harassment
- Slander
- Defamation
- Obscene or suggestive message(s) or offensive graphical images(s)

Department or agency directors may establish within their departments stricter remote access use policies and/or regulations in addition to those recommended in this document.

The signed document will be given to the Technology Services team responsible for maintaining the user account and a copy will be forwarded to the department that owns the RAS or VPN system that will be used for remote access.



## Statement of Responsibility

As an approved User of the City and County of Denver's ("City") IT infrastructure, I will protect the stated and implied interests of the City, and I will abide by the terms and conditions for the issuance of a User identification code (UserID) and password as stated below. I will protect all City-related information that would jeopardize the security or financial position of the City or that might violate an individual's privacy. I will use the system resources, regardless of the type of system responsibly and only for the purposes the City has intended. I realize that I am responsible for all activity done using my UserID on any City system. I am aware that deliberate misuse of any City system or City information is a breach of trust on my part.

If I release information either inadvertently or as a result of correcting an emergency situation, I will take corrective measures as soon as possible and immediately report the incident to management.

### **Additional Terms and Conditions for Issuance of UserID and password:**

- The granting or denial of remote access privileges are maintained by network administrators at both the local level and the enterprise level. Access privileges may be revoked at any time when a network administrator finds it necessary to protect the network from security risks or maintain proper use of remote access.
- It is the responsibility of the person using remote access to keep their passwords confidential. If the User gives a password or access to any other person, whether accidentally or otherwise, the User may be deemed solely or jointly responsible for misuse of the access privileges with the person actually misusing the system.
- Sharing UserIDs and Passwords is NOT allowed, and constitute unauthorized use of City resources. This may result in access privileges being removed from the original user without notice, and could be grounds for disciplinary action, including dismissal from employment.
- If the User suspects that someone may have obtained the password, or logged in with their UserID by any means, the User will immediately change his/her existing Password. In addition, the User must notify the Help Desk immediately if there is reason to suspect possible misuse of their UserID, password, and related access privileges. The Help Desk will escalate the issue to the Technology Services Security Administrator for additional review and action.
- The User, User's immediate Supervisor and Department management share the responsibility for immediately notifying the responsible Help Desk, IT support Group, or Security Administrator of any changes in User status from, but not limited to: ceasing employment with the City, name change (or misspelling), transfer to another department or agency, changes in User responsibilities which would alter the access privileges required, or the existence of multiple UserIDs for a single individual.
- The City reserves the right to read any files of documents stored upon City-owned equipment.

- The User will not knowingly load a virus onto any City computer.
- Violations of this policy by City employees can result in disciplinary action up to and including dismissal for a first offence, in accordance with the City's Personnel Rules, and other applicable Administrative Regulations, as well as any department rules, policies, or regulations.
- Violations of this policy by non-City employees granted special access to the City network can result in the revocation of their access privileges and/or termination of their business relationship with the City.
- The User must provide appropriate security at their remote (home or work) site including updated anti-virus software, must not have a "split tunnel" configuration (see definition below), and those installations with Cable/DSL/T-1 or other high speed connections must have a firewall.
- All department rules which define operating procedures and provide rules and limitations on the use of City computer equipment also apply to out of the office use.
- By signing this agreement the applicant for access privileges (User) accepts all terms of this agreement and consents to the City taking any and all measures to insure the User is in compliance with this agreement.

**Definitions:**

- *Split Tunnel Configuration*: where a computer that is accessing the City's network is, itself accessible on the internet. Most Cable/DSL connections are configured this way. Check with your network administrator on how to block this.
- *Firewall*: a software and/or hardware product that protects your computer/network from internet attacks.

**Adherence to the above Statement of Responsibility, and to the terms and conditions for remote access, are a condition of my continued employment by the City. The City may change this agreement at any time.**

\_\_\_\_\_  
\*Printed Employee/User Name      \*Signature of Employee/User      Date

\_\_\_\_\_  
\*Department/Agency - Printed      \*Signature of Immediate Supervisor      Date

\*Operating system at home \_\_\_\_\_

\*Computer name at work \_\_\_\_\_

**\* THE ABOVE FIELDS MUST BE COMPLETED TO PROCESS THIS FORM**