



Complete all required fields on this form (as indicated in **\*red**). **SUPERVISOR SIGNATURE REQUIRED.** (Note: Digital Signatures are preferred. For more information on creating a digital signature( [<Click Here>](#)). Forms submitted without supervisor's signature will be returned. New CDOT State Employees email the form to [dot\\_workforce\\_staffing@state.co.us](mailto:dot_workforce_staffing@state.co.us). All others email the form to [OIT\\_ServiceDesk\\_CDOT@state.co.us](mailto:OIT_ServiceDesk_CDOT@state.co.us). If you have questions, call the Service Desk at 303-757-9317. Please understand if the form is incomplete or unclear, it may cause a delay with processing the request. OIT will make every effort to process the request within five(5) business days after receiving the correctly completed form.

**Request Type:**  New User Account  Modify Account  Delete Account  Transfer Account  Name Change  
 Google Group  Shared Mailbox  Google Calendar  Security Group/Directory  Service Account

If multiple agency access is requested, specify home agency/primary account location:

**\*Need by Date:** \_\_\_\_\_ **\*Submission Date:** \_\_\_\_\_

**Applications Requested** (Select all that apply)

SiteManager	Preconstruction(Web Trns*port)	CARS	Permits	Mill/Asph	SAP/ERP
ProjectWise	Project #	Sharepoint	VoiceMail	Ext#	VPN

**Employment Status:** Permanent Temp (# of mos/last day):  
 Perm PT Seasonal Perm PT Intern

Consultant Contract/PO # Contract Exp Date:  
 Current State Employee needing dual agency access

**EMPLOYEE INFORMATION** (Complete all fields in the following section with current information.)

*Last Name:		*First Name:		*MI:	If account exists enter Network Username
*Agency Name:	*Region	*Division		Job title/Position:	
*Business Address (permanent work location):			Business Phone Number:		Employee Email Address:
*Direct Supervisor Name:		*Direct Supervisor Phone Number:		*Supervisor/Consultant Firm Signature:	

Please provide any additional information regarding requests, service accounts, groups, Google or directories:

For employee **deletions**, specify task for Google mail: Delete Mailbox Delegate Access to  
\*For employee **deletions**, transfer Google Drive and Docs to:

For employee transfers, list name of region user is leaving and region user is transferring to.

From Region: To Region: OR From Agency: To Agency:

For employee name change, list previous name and new name.

Previous Name: ID: New Name:

**Google User accounts, Shared Mailbox, Groups or Resources**

User Account - By default, new user account will be added to the appropriate region "All Employee" Google Group. If this should not occur, specify that in the "Additional Information" field. All other groups are maintained by the manager of the group.

Shared Mailbox  Group  Resource

Shared Mailbox proposed name: dot\_ Owner:

Group proposed name:cdot\_ Manager:

Resource Type: Calendar Room Vehicle IT Equipment

Physical Address of the resource:DOT - Managed By:

**Domain Administrator Account Request:** \*requires justification (insert below) and 5i h.cf]nYX'5ddfcj Yf signature

"

Authorized Approver Signature:

Date:

**Additional Security Group Requests:** \*requires approver signature before submission

Group Name: Authorized Approver:



## Statement of Compliance

(To be read and signed by the employee on a NEW request or Name Change)

### Terms and Conditions:

- CDOT's information or communication systems must be used in a responsible, lawful and ethical manner. Usage for personal or unauthorized activities is strictly prohibited and could result in criminal prosecution under applicable state and federal laws. CDOT's information technology, Internet access and communication systems must be used solely for purposes that serve CDOT's mission and goals, and must be accessed only with a valid computer account or long distance access code.
- You should have no expectation of privacy, rights or ownership in anything you may access, create, store, send, or receive within CDOT's network. This application constitutes your waiver, and consents to monitoring, retrieval and disclosure of any information in this network, for all purposes deemed appropriate by CDOT, including the enforcement of agency rules.
- OIT creates an audit log detailing every inbound/outbound connection made to the Internet, or through the phone system.
- Access Control assigns unique usernames and passwords to each account holder. You may not share your password with any other individual. Passwords must be a minimum of 8 characters long and expire on a regular basis. You will therefore be required to reset your password on a periodic basis and must assume full responsibility for the security of your password.
- Access codes for long distance dialing are issued to authorized employees and must be kept private. Sharing of long distance access codes is prohibited.
- You must be responsible when using information and communication systems, and not take any action that interferes with voice or data network operations or with the work of other network users.
- You are responsible for the secure handling of sensitive personnel, financial and/or security related information you may be authorized to handle, and conform to the Colorado Cyber Security Policies for Data Handling and Disposal.
- Accessing, viewing, downloading, e-mailing, or storing pornography is strictly prohibited. Pornography is considered sexual harassment at CDOT and will not be tolerated.
- Downloading or installing software that has not been approved by OIT is prohibited. Software must be used in accordance with applicable licensing. Installing software without a valid license is prohibited.
- Transmission of material in violation of any state or federal law or regulation is prohibited.
- Dissemination of information regarding CDOT's network, network topology, network addressing or hardware is prohibited.
- Unauthorized activities that could compromise the Department's systems or data are strictly prohibited, including: network scanning (sniffing), vulnerability scanning, security testing, and password cracking.
- Attempts to defeat security mechanisms are treated as a security incident and are potentially subject to civil and/or criminal penalties. You should report to your supervisor, any observed attempts by others to defeat security mechanisms.
- You are responsible for maintaining full and up-to-date virus protection on any microcomputer used to access the Information Interchange network. All downloaded files must be isolated and checked for known viruses before use.
- Internet access, Internet email and external voice communication depend on the configuration and availability of systems beyond CDOT's network, and are outside the control of OIT or the Colorado Department of Transportation.

### E-mail Terms and Conditions:

- You must use email solely for business-related communications. Abuse of email may lead to suspension of your computing privileges and possible disciplinary action.
- Email to a large number of accounts at one time is not allowed without prior permission. Employees without system-wide distribution privileges may submit messages to the Service Desk or Public Announcements for widespread distribution.
- You can attach documents and other objects to Internet messages.
- Chain mail is prohibited within CDOT. Please do not forward chain letters, games, virus alarms, or solicitations for donations. These are non-productive in the CDOT work environment.
- Do not use your CDOT email address for non-related business activities such as receiving correspondence from commercial websites, participating in news groups, instant messaging, or any other activity resulting in receiving non-business related email.

**Statement of Understanding:** I've read the above Acceptable Use Policy and agree to abide to the terms and conditions. I understand that any violation of these Terms and Conditions may result in suspension and/or termination of my access to Information Interchange and/or the Internet. In addition, OIT may make recommendations to the Director of the Division of Human Resources and Administration for further personnel actions. Restored access to the CDOT network will require written explanation along with signature approval from the user's Division Head or Region Transportation Director.

**\*Employee signature:**

**\*Date:**

**User must provide two unique words (This information is used solely to verify User's identity for resetting passwords):**

**\*Unique Word 1:**

**\*Unique Word 2:**

---

My signature below certifies that the above applicant is a CDOT employee/Consultant under my supervision, and that I am responsible for ensuring that this applicant understands the information in this Access Request Form, and that I am responsible for notifying the Service Desk when this applicant leaves employment at CDOT, or transfers to a position which I do not supervise.

**\*CDOT Supervisor signature:**

**Date:**