



Complete all required fields on this form (as indicated in **\*red**). **SUPERVISOR SIGNATURE REQUIRED**. (Note: Digital Signatures are preferred. For more information on digital signatures or how to create one [<Click Here>](#) Forms submitted without the supervisor's signature will be returned. Email the completed 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:

**\*Effective Date:** \_\_\_\_\_ **\*Submission Date:** \_\_\_\_\_

**\*Employment Status:** Permanent Temp (# of mos\last day): PPT\Seasonal Perm PT Intern  
Contract PO # \_\_\_\_\_  
Current \_\_\_\_\_

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

|   |                |   |                               |   |                                      |
|---|----------------|---|-------------------------------|---|--------------------------------------|
| <b>*Last Name:</b>                                  |                | <b>*First Name:</b>                     |                               | <b>*MI:</b>   | <b>If existing account -Username</b> |
| <b>*Organization Name:</b>                          | <b>*Region</b> | <b>*Org Unit #HR (SAP) Position</b>     | <b>Job Title/Description:</b> | Employee ID or 2 Unique words used when requesting a password reset |                                      |
| <b>*Business Address (permanent work location):</b> |                |   | <b>Business Phone Number:</b> | <b>Employee Email Address:</b>                                      |                                      |
| <b>*Direct Supervisor Name:</b>                     |                | <b>*Direct Supervisor Phone Number:</b> | <b>Supervisor Signature:</b>  |   |                                      |

**Applications Requested:**

|   |               |          |
|---|---------------|----------|
| SiteManager <b>*must submit a SiteManager Access Agreement form with this form (click here)</b> | Permits       | CARS     |
| ProjectWise <b>*include Project #</b>   | Web Trns*port | MillAsph |
| SharePoint <b>*include URL</b>  | VPN           |          |
| SAPIERP <b>*must submit an ERP Authorization Request Form (#1387) - (click here)</b>            | VoiceMail     |          |

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

For employee **deletions** or transfers, specify task for home directory files: Delete Files Copy Files To  
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 tgi kqp "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:

**Administrator Account Request: \*requires justification (insert below) and ISO signature before submission**

**\*ISO Signature:**

**Date:**

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

Group Name:  Authorized Approver:

## Statement of Compliance

### 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 e-mail 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 e-mail solely for business-related communications. Abuse of e-mail may lead to suspension of your computing privileges and possible disciplinary action.
- E-mail 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. To control network traffic however, do not attempt to transfer messages or attachments larger than 25MB (aggregate.)
- 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 e-mail 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 e-mail.

### Wireless Terms and Conditions:

- WiFi access is provided in conference rooms at main regional sites as a convenience, and should not be expected to provide the same quality of service and reliability as the hardwired network. Always use the hardwired network when performance and reliability are critical.
- WiFi support from OIT will be limited to CDOT WiFi locations only.
- Unapproved devices that disrupt extend, or rebroadcast wireless access will be confiscated and the device owner will be subject to disciplinary actions.
- Employees seeking wireless connectivity to CDOT's network must attend training and must use authorized software that restricts wireless access to a secure connection with only CDOT's network, per IT Standard Operating Procedure #1010.

**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.

|   |                                |             |
|---|--------------------------------|-------------|
| <b>Employee signature</b>   | <b>Title</b>                   | <b>Date</b> |
| <p><b>"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 the herein Access Request Form, and that I am responsible for notifying the Service Desk when this applicant leaves the employment CDOT, or transfers to a position which I do not supervise."</b></p> |                                |             |
| <b>Supervisor signature</b>   | <b>Supervisor Name (print)</b> | <b>Date</b> |