



Supervisors complete all required fields on this form (indicated by * red fields). **Supervisor signature is required.** Forms submitted without the supervisor's signature will be returned. Email the completed form to OIT_ServiceDesk_CDPHE@state.co.us. If you have questions call the Service Desk at (303) 692-2266. 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 5 business days after receiving the properly 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 Temporary/Seasonal *End date if applicable* MM/DD/YYYY
 External Contractor Intern Vendor Current State Employee needing dual agency access

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

*Last Name:		*First Name:		*MI or N/A:	If existing account -Username
*Agency/Institution:		*Division/Section:		*Job Title and Level:	
				* Two Unique Identifier words used when requesting a password reset:	
*Business Address and room number:			Business Phone Number:		Employee Email Address:
*Supervisor Printed Name:		*Supervisor Phone Number:		Supervisor Signature:	

Please provide any additional information regarding network access requests, service accounts, groups, mailboxes or directories:

For employee **deletions** specify task for home directory files: Delete Copy Files to:
For employee **deletions** specify task for Google mail: Delete Delegate 30 day access to:
For employee **deletions** transfer ownership of Google Docs to

For employee transfers, list name of division user is leaving and division user is transferring to.
From Division: To Division: OR "" From Agency: To Agency:
For employee transfer specify task for Google mail: No Action CDPHE Retains All Inbox Contents

For employee name change, list previous name and new name. Has HR been notified? Yes No
Previous Name: ""ID: ""New Name:

Google User accounts, Shared Mailbox, Groups or Resources
 User Account **By default, new user accounts will be added to the appropriate "All Employee" Google Group. If this should not occur please specify in the "Additional Information" field on Page 1.*
If you have different first name you prefer, OIT will attempt to use it to create your email address.
Preferred Name:
 Shared Mailbox Group Resource
Shared Mailbox proposed name: cdphe_ @state.co.us
(Password will be provided to employee listed on page 1)
Group proposed name: cdphe_ @state.co.us
(Manager will be employee listed on page 1 unless specified otherwise)
Resource Type: Calendar Room Vehicle IT Equipment
Physical Address of the resource: Managed By:

Remote Access
 VPN COFRS codes
Justification:
Approver Signature:Date:

Additional Applications Requested:

.....f'D'YUgY'cVHJ]b'h Y'U' h cf]nYX'Uddfcj Yfg'g][bUhi fY'Z:f'h Y'Udd']WU]cb'fYei YghX'VYZ:fY'gi Va]H]b['Z:f'UWVYgg".....

Notes

Authorized Approver Signature

Aspen_Only

Cedrs

Covis (location)

Covis (group)

Death Index

eCars

eCast

FTP (path)

HMD_GIS

Lits+

Refugee Database

Tbdb

WebPlus (role)

WebPlus(location)

Zoonosis

Other

Statement of Compliance

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

It is the policy of this agency that the Executive Order, dated July 1, 1978, and the former Division of ADP Policy Statement regarding access of public records through the use of computer technology be strictly adhered to. It is the public policy of this state that all public records shall be open for inspection by any person at reasonable times, except as provided in Part 2 of Article 72 of Title 24, CRS 1973 as amended, or as otherwise specifically provided by law.

The release of any information to the public, supplied through automated processes, shall not take place unless the following events have transpired:

- Written requisition delineating the desired information, records, or data must be received by the official custodian.
- The official custodian must determine if the requested information, record, or data constitutes public record and its disclosure is within the law.

All data resulting from the activities of an agency using ADP equipment is considered private data of that agency. Use and dissemination of this data is absolutely prohibited without proper authority being given. The appropriate Executive Director or the official custodian must provide written authority to the computer facility director prior to any data within the facility director's jurisdiction being released in any manner to any individual, government agency, or private concern. It is the facility director's responsibility to adopt adequate safeguards to protect data stored within the facility.

End User System Access and Acceptable Use policy

The integrity of the organization's data is of prime importance. The following terms and conditions are intended to protect OIT information and communications from unauthorized access, in accordance with the State of Colorado Cyber Security Policies.

Issuance of your account is predicated upon your acknowledgement, acceptance and adherence to these items.

Terms and Conditions:

OIT 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. OIT information technology, Internet access and communication systems must be used solely for purposes that serve OIT mission and goals, and must be accessed only with a valid computer account.

You should have no expectation of privacy, rights or ownership in anything you may access, create, store, send, or receive within OIT 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 OIT, including the enforcement of agency rules.

Employee acknowledges that confidential information and/or reports will not be copied or discussed with family members, friends, professional colleagues, other employees, clients/customers, or any other person unless such person has been authorized to access that information. If unsure who is authorized to access the information, employee will check with their direct supervisor or the point of contact responsible for the information.

Any violation of federal, state, assigned agency or the program's confidentiality requirements or this Agreement will be considered a breach of obligations and may result in disciplinary action, up to and including termination of employment, termination of contractual relationship and other remedies allowed by law during or after my employment per the State of Colorado Personnel Rules.

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.

Transmission of material in violation of any state or federal law or regulation is prohibited.

Downloading or installing software that has not been approved by the OIT is prohibited; this includes P2P software, Internet Browser plug-in, screen savers, PDA synchronization software, and encryption software. Software must be used in accordance with applicable licensing.

For audit or system security purposes, OIT may monitor all activity conducted on state equipment, during and after business hours.

Unauthorized activities that could compromise OIT systems or data are strictly prohibited. These activities include but are

