COLORADO
Governor's Office of Information Technology

Colorado Department of Transportation

Access Request Form

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. New CDOT Employees email the form to dot_workforce_staffing@state.co.us. Other requests email the completed form to OIT_ServiceDesk_CDOT@state.co.us. If you have questions call the Service Desk at 303.239.HELP(4357). 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 correctly completed form. For new employee access submit the request two weeks prior to the Need By Date.

***Need By Date:** 08/08/2016 ***Submission Date:** 08/01/2016

Onboarding Request - Select all that apply: (If transferring from a State Agency or Division also complete Transfer section on Page 2)

☐ New User Account ☐ Google Email Account ☐ Desk Phone ☐ Computer

Applications - Select all that apply: (Note: Some access may require additional information as noted)

Click here to specify request type

☐ Mill/ASPH ☐ SiteManager/CAR ☐ Preconstruction(Web Trns*port) ☐ CARS(State Vehicle Tracking)

☐ Permits ☐ SAP/ERP ☐ ProjectWise - Project # ☐ SharePoint

☐ VoiceMail Ext #

Access Request - Select all that apply: (Note: Some access may require additional information as noted)

Add Application Access - Select applications that apply - Complete application sections on Page 2

☐ Service Account ☐ Security Group/Directory

☐ Google Group (Complete Google section on page 2) ☐ Database Access

☐ Google Resource (Complete Google section on page 2) ☐ VPN Access

☐ Google Shared Mailbox (Complete Google section on page 2)

Offboarding Request - Select all that apply: (Note: Some access may require additional information as noted)

Click here to specify deletion or transfer

Specify Delegation or deletion of Google Email To:

Specify transfer of Google Drive and Docs (Supervisor will receive if left blank) To:

Employment Status: Full Time/Staff Contract PO #:

End Date:

☐ Current State Employee needing dual agency access - Specify Home Agency: Select Agency

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

*Last Name:	*First Name:	*MI:	If account exists - list Network Username:
Hays	Bryon		Bhays

*Agency:	*Region	*Division/Section:	Job Title:
CDOT	HQ	HR\OED	Trainer

*Business Address:	Business Phone Number:	Employee Email Address:
4201 E Arkansas Ave, Room 290	303-757-9726	bryon.hays@state.co.us

*Supervisor Name:	*Supervisor Phone Number:	Supervisor/Consultant Firm Signature:
Morgan Murphy	303-757-9684	

Active Directory Security Groups or File Shares

Group Name: Approver Signature:

Group Name: Approver Signature:

Group Name: Approver Signature:

Database Access - Select all that apply:

☐ Window ☐ Mixed Mode

Google Shared Mailbox, Google Groups or Resources Google Shared Mailbox, Google Groups or Resources

Shared Mailbox proposed name: Owner:

Group proposed name: Manager:

Resource Type:

☐ Calendar ☐ Room ☐ Vehicle ☐ IT Equipment

Physical Address of the Resource: Managed By:

For employee name change, list previous name and new name. Has HR been notified? ☐ Yes ☐ No

Previous Name: Current User ID: New Name:

For employee transfers, list name of Division or Agency user is leaving and Division or Agency transferring to.

From: Click here to select To: Click here to select

SiteManager Account Type/Security Group - Select All that apply (CAR SAP reporting is given by default)

Construction:

☐ CDOT Project Engineer ☐ Consultant Project Engineer ☐ Manager Read-Only ☐ Resident Engineer

Materials:

☐ Region Materials Office ☐ Consultant Sampler/Tester ☐ Sampler/Tester ☐ Central Lab

Region: . SiteManager Training Date(Month/Year):

CDOT Res Engineer Printed Name:

CDOT Res Engineer Authorization Signature: Date:

SAP

Select here to specify type of access

End Date:

CDOT Employees: All SAP Roles are given to employees by way of their position number. You should have all the roles you need without submitting this form.

Non-CDOT Employees (Contractors and OIT Staff): All Contractors that request access to SAP will receive a composite role (RXITO_COMP), which includes display access to most areas of SAP.

All: If there is specific access you think you need and do not have, please contact the appropriate BPX http://intranet/resources/sap/sap-team/business-process-experts-bpx to discuss further. If you need to coordinate with multiple areas or have any questions, you can contact the Business Process Architect http://intranet/resources/sap/sap-team/overview.

Additional roles being requested after discussion with the appropriate BPX:

Web Developer role. Requesting access to \\hqbetawebcs\betaexternal\content\programs\training\

Justification/Comments(You must enter a justification when requesting additional roles for a position):

Trainers need the ability to test web enabled content.

VPN Access (Provide justification and approval signature below)

Authorized Approver signature:

Provide any additional information regarding the request, service accounts, groups, Google or directories:

COLORADO
Governor's Office of Information Technology

Statement of Compliance

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

In a commitment to transparency in government, the Colorado Open Records Act (CORA), C.R.S. 24-72-201 to 206, provides that all public records shall be open for inspection by any person at reasonable times, except as otherwise provided in Part 2 or as otherwise specifically provided by law. It is the policy and expectation of this agency that all employees shall strictly adhere to the provisions of CORA as well as your agency's CORA policy, if any.

CORA provides that 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 state-owned 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.

System Access and Acceptable Use Policy

The integrity of the organization's data is of prime importance. All state IT resources, information, and data are the sole property of the State of Colorado and applicable statutes, policies and guidelines govern their use. The following terms and conditions are intended to protect the State of Colorado's data, and information and communications systems from unauthorized access, in accordance with the State of Colorado Cyber Security Policies, Acceptable Use of State & Personal Assets Policy POL 100-11 (AUP), and your agency's Acceptable Use policy, if any.

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

Per State Personnel Board Rule R-1-162, "It is the duty of state employees to protect and conserve state property. No employee shall use state time, property, equipment, or supplies for private use or any other purpose not in the interests of the State of Colorado."

State 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. State information technology, Internet access and communication systems must be used solely for purposes that serve state and/or agency 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 the state's network. This application constitutes your waiver and consent to monitoring, retrieval and disclosure of any information in the network for all purposes deemed appropriate by your agency or the Governor's Office of Information Technology (OIT), including the enforcement of agency rules.

You are responsible for cooperating with the state Chief Information Security Officer (CISO) or designee during any investigation of misuse of state information equipment, data or other violations of this compliance and policy document.

You acknowledge 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 your 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/or other remedies allowed by law during or after your 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 must conform to all related state and agency policies.

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 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 state systems or data are strictly prohibited. These activities include but are not limited to: network scanning (sniffing); vulnerability scanning; security testing; and modification of IP, proxy, DHC, DHCP, and other such settings; and password cracking.

Each account holder is assigned a unique usernames and password to access the network, systems and/or applications. You may not share your password with any other individual. Passwords must be a minimum of nine (9) characters, include a combination of alphanumeric characters, upper and lowercase 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.

By signing this form you agree to access only the information you need to do your job, and not to access or attempt to access files you are not authorized to use. You will not "browse" or otherwise use files or programs that exceed what is the minimum necessary to do your job. Your use and disclosures of information will be consistent with those permitted by applicable state and federal laws and rules.

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.

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.

Chain mail is prohibited; Do not forward chain letters, games, virus alarms, or solicitations for donations.

Do not use your state e-mail address for non-related business activities such as receiving correspondence from commercial websites, participating in newsgroups, instant messaging with non-state employees, or any other activity resulting in receiving non-business related e-mail.

Internet Terms and Conditions:
Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner.

All Internet access is used for authorized purposes only and that Internet use is for valid business reasons.

Inappropriate use of the Internet is not allowed and will not be tolerated. Prohibited practices include:

- Visiting Internet sites that contain offensive, obscene, pornographic, hateful and/or other objectionable

materials; send or receive any material, whether by email, voice mail, memoranda or oral conversation, that is obscene, defamatory, harassing, intimidating, offensive, discriminatory, or which is intended to annoy, harass, or intimidate another person.

- Playing games, gambling, sports, entertainment and/or streaming audio or video material not beneficial to the state.
- Posting news to newsgroups, use of chat facilities, social networking sites, and participation in mail lists except as authorized by your agency policy, if any.
- You shall not make unauthorized purchases or business commitments through the Internet that are not related to state business.

By signing this, you acknowledge that you are responsible for ensuring that your subordinate has read, understands, and agrees to the AUP and all other security policies as a condition of employment or a condition for granting access.

*Supervisor 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:

*Employee Signature: Date: