



COLORADO
Department of Public Safety

December 22, 2023

Staff of the Legislative Council
State Capitol Building
200 East Colfax
Denver, Colorado 80203

Dear Staff of the Legislative Council:

In accordance with Section 24-72-204.5(3), C.R.S., I am pleased to present this report outlining the Department of Public Safety's electronic mail retention policy.

Statute requires the submission of a report outlining the department's policy to the staff of the Legislative Council of the General Assembly on or before January 1, 2024.

The Department of Public Safety's email retention policy is attached.


Sincerely,

Stan Hilkey, Executive Director



COLORADO

Department of Public Safety

<p>Title: IT Acceptable Use Main Section: Department Sub Section: Information Technology</p>	<p>POLICY NUMBER: 1.09.003 VERSION: 1.3 Supersedes: Use of Electronic Messaging Systems (Email) 5.2.2</p>
<p>Related Mandates, Law, Standards, Executive Orders, Policies, or Procedures: C.R.S. §24-72-204.5; Governor’s Office of Information Technology’s Acceptable Use of State Data & IT Resources policy, P-CISP-018; FBI CJIS Security Policy version 5.7.</p>	
<p>APPROVED BY:  EXECUTIVE DIRECTOR</p>	<p>January 17, 2023 EFFECTIVE DATE</p>

I. BACKGROUND AND PURPOSE

The use of information technology resources, including access to email, the internet, state applications, networks and systems, etc. is a privilege that enables Colorado Department of Public Safety (CDPS) employees to perform their jobs efficiently, and it is incumbent upon each user to ensure that these resources are used in a responsible and ethical manner that is compliant with all state and federal laws and applicable policies.

The purpose of this policy is to establish rules and standards for securing CDPS data, networks, and systems. These standards are necessary to minimize both unauthorized access/use and to preserve the integrity of the Department’s confidential information, personally identifiable information (PII), and Criminal Justice Information (CJI).

II. SCOPE

This policy applies to all CDPS employees and other users that operate, create, manage or support CDPS’s network resources and email system(s).



COLORADO

Department of Public Safety

III. DEFINITIONS

- A. **User:** A State of Colorado employee, temporary worker, contractor, intern, volunteer, third-party vendor, or any other individual who has been granted access to CDPS's email system(s) and IT network(s).
- B. **CDPS Business Sponsor:** A CDPS employee that is responsible for CDPS projects and programs and that sponsors users who are not CDPS employees for the purposes of obtaining specific systems access necessary for conducting State business.
- C. **CDPS IT Access Administrator:** Local CDPS employees classified as an IT professional with expertise in access control.
- D. **Criminal Justice Information (CJI):** Any and all data provided through CBI-CJIS Systems, to include biometric, identity history, biographic, property, and case/incident history data obtained from the FBI's National Crime Information Center (NCIC) database, the CBI's Colorado Crime Information Center (CCIC) database, Criminal History Record Information (CHRI), the International Justice and Public Safety Network (Nlets), the CBI Secure Document Delivery System (SDDS), and/or the FBI National Data Exchange (N-DEx).
- E. **Criminal Justice Information Services (CJIS):** CJIS refers to the FBI's Criminal Justice Information Services Division.
- F. **CJIS System:** Any information system or subpart, to include any network, storage device, or application designed and/or intended to contain CJI and/or information derived from CJIS, including data in servers, databases, CJI repositories, and the CDPS Network that provides access to CJI.
- G. **CDPS Network:** Local access and connection to the CDPS infrastructure by way of computers, servers, mainframes, and/or devices to share/access internal data and electronic communication.
- H. **CDPS Wireless Network:** Main CDPS Network wireless solution designed for employees to access the CDPS Network and all resources. This wireless SSID (Wireless Connection Name) is CDPS-GOV.
- I. **CDPS Guest Wireless:** CDPS guest wireless network connection designed to provide wireless internet access to authorized guests of CDPS facilities providing no access to CDPS resources. This wireless SSID (Wireless Connection Name) is guestwifi.
- J. **CDPS Emergency Operations Center Guest Wireless:** A wireless network connection designed for visitors of the Emergency Operations Center to be used during an emergency activation providing internet



COLORADO

Department of Public Safety

access. This wireless solution provides no access to CDPS resources. This wireless SSID (Wireless Connection Name) is EOCGuest.

- K. **Email System(s):** The systems and/or applications CDPS utilizes for emailing, including CDPS email that can be accessed from personal devices. Currently CDPS uses Google Gmail as the electronic mail application.
- L. **Public Wi-Fi Networks:** Unsecured, non-CDPS, public Wi-Fi networks, such as in cafes, restaurants, libraries, airports, hotels, or other public areas.
- M. **Unapproved devices:** Network infrastructure devices connected to the CDPS network for business or non-business purposes that were not approved by the employee's supervisor and/or not installed or configured by CDPS IT personnel, such as personal devices or equipment or those purchased outside of the procurement process and including, but not limited to, wifi extenders and other devices, personal phones, iPads, laptops, and printers.

IV. POLICY

- A. CDPS's network, Internet/Intranet access, and email systems, and all email messages within are the sole property of the State of Colorado, and applicable statutes, policies, and guidelines govern their use.
- B. The terms and conditions for use of CDPS's network including Internet/Intranet access and email systems are in accordance with the [State of Colorado Information Securities Policies \(CISPs\)](#), [Acceptable Use of State Data & IT Resources \(AUP\)](#), State Board Rule 1-16, C.R.S. §24-72-204.5, and the [FBI-CJIS Security Policy](#) (where applicable), all of which are intended to protect the State of Colorado's data and information in communications systems from unauthorized access. As part of the system access request process, issuance of employee and other user accounts are predicated upon the acknowledgement, acceptance, and adherence to these terms.
- C. CDPS has the right to monitor and/or investigate any user's network and email account and their usage for legitimate business reasons, whether on state-issued equipment or personal devices.
- D. Users have no expectation of privacy when using the CDPS network including Internet/Intranet access and email system(s). All electronic communications including, but not limited to, email, text messages, instant messages,



COLORADO

Department of Public Safety

and any other forms of electronic communication sent to and from State-assigned accounts are the property of the State.

- E. Electronic communications pertaining to State business are subject to the Colorado Open Records Act (CORA) C.R.S. §24-72-201, *et seq.* and the Criminal Justice Records Act (CJRA) C.R.S. §24-72-301, *et seq.* Any communication made using personal devices is also subject to CORA and CJRA to the extent it pertains to State business. Any individual using a personal device for State business is responsible for searching the personal device or account in response to any request for records under CORA.
- F. Use of CDPS's Internet/Intranet access and email system(s) is for the purpose of conducting official State business. Limited personal use of CDPS system(s) is permitted but discouraged due to the proliferation of cybersecurity threats. Any personal use must comply with this policy, is subject to the legal discovery process, must not interfere with work duties, and is at the user's own risk. The State is not responsible or liable for any personal data that employees choose to transmit over State IT resources.

V. PROCEDURE

A. Network and Email Systems Security

1. Due to cyber security threats, CDPS users are prohibited from connecting any unapproved devices to the CDPS network, either by plugging a CDPS network cable into the personal device or by using the personal device to connect to the CDPS Wireless Network (SSID "CDPS-GOV").
2. CDPS employees shall not access CJIS Systems or store CJI on anything other than a State-issued device that has the appropriate mobile device management (MDM) measures in place as prescribed by the CJIS Security Policy.
3. Logging into State Gmail or other Google Suite applications on a personal device is permitted as long as users connect to the internet using something other than the CDPS Wireless Network, such as a user's personal cellular telephone network.
4. Authorized users may connect a personal device to the CDPS Guest Wireless Network (SSID "wifiguest") and/or the Emergency Operations Center Guest Wireless Network (SSID "EOCGuest") at



COLORADO

Department of Public Safety

applicable CDPS facilities for approved business purposes, excluding access to CJIS Systems through those networks.

5. Any unauthorized access to sensitive data, confidential materials, documents and files of CDPS business, including PII or CJ, on a personal device is subject to the protection regulations under C.R.S. § 24-73-103 regarding security breach notification requirements.
 6. Any unauthorized access to CJ data or CHRI on a personal device is subject to the [FBI-CJIS Security Policy](#) and to Personnel Rules and State and Departments policies.
- B. Access Grants and Termination
1. No network access, change or deactivation will be granted without a request from a CDPS supervisor or CDPS Business Sponsor submitted to OIT using a Help Desk Ticket via the OIT Customer Service Portal, via phone 303.239.HELP (4357), or through email to oit_servicedesk_cdps@state.co.us.
 2. The CDPS supervisor or CDPS Business Sponsor determines and reviews access requests based on business needs. CDPS IT Access Administrators will ensure proper controls for system(s) access.
 3. CDPS supervisors and CDPS Business Sponsors are responsible for working with CDPS IT Access Administrators to create accounts, disable accounts, transfer accounts, allow temporary access, identify licensing and software placement, and change or update applications, database platforms, directory groups, file sharing, and/or any security group access accounts.
 4. Network and Email Account Creation Requests
 - a. The CDPS supervisor or CDPS Business Sponsor for each new user will request the creation of account(s) by submitting an OIT Help Desk Ticket at least two weeks prior to the employee/contractor's start date.
 5. Network and Email Account Change Requests
 - a. The CDPS supervisor or CDPS Business Sponsor for each user may request changes to accounts by submitting an OIT Help Desk Ticket.
 6. Network and Email Account Disable Requests
 - a. The CDPS supervisor or CDPS Business Sponsor for each separating user shall submit an OIT Help Desk Ticket request to disable or to emergently disable the accounts of a separating user.
 - i. The Help Desk Ticket should be submitted at the same time the CDPS 5 is created, if applicable. CDPS Human Resources



COLORADO

Department of Public Safety

will assist in this procedure by notifying the CDPS supervisors or CDPS Business Sponsor of their options. (See [Classified Employee Transfer/Separation Checklist](#)).

- b. Failure to submit an OIT Help Desk Ticket may result in an IT Access Administrator monthly reporting error that may result in the user's account access being disabled.
7. Emergency Network and Email Account Disable Request
 - a. A CDPS supervisor or CDPS Business Sponsor shall request the emergency account(s) termination by submitting an OIT Help Desk Ticket and immediately following up with a telephone or email request to the CDPS IT Director.
 - b. The CDPSIT Director will verify the emergency disable request with the CDPS Executive and/or the CDPS Chief Human Resources Officer prior to disabling the account.
- C. Email and Systems Use and Etiquette
 1. Users are expected to use common courtesy in emails and never send messages that are detrimental to the Department.
 2. CDPS requires all employees to use a standardized email signature in all internal or external communication related to CDPS in accordance with Brand Colorado State branding guidelines as directed in the [DPA Digital Guidelines](#). This signature identifies the sender's name and position in the Department while maintaining credibility. In addition, this signature represents CDPS and helps maintain a clean, cohesive brand.
 - a. Email signature typesetting format should use Trebuchet MS font, normal size, black color text, bold text weight for name and title, and regular weight for all other text.
 - b. Email signature should follow the linear format:
First line (bold font): **First name, Last name**
Second line (bold font): **Title**
Third line (regular font): Work unit name (optional)
 - c. Logos: State of Colorado/ Department Logo - vertical bar -
COLORADO
Department of Public Safety (under Colorado) with Alt Text added
 - d. Phone contact: Work ###.###.#### vertical bar Fax (if applicable)
vertical bar Cell ###.###.####
 - e. Work Address (optional) on a single line
 - f. State email hyperlinked



COLORADO

Department of Public Safety

3. To comply with accessibility standards, Alt Text should be added to any images, including the CDPS logo, used in email signatures to describe the image or the function that the image serves. To add Alt Text to the image and/or CDPS logo:
 - a. Open a new document in Google Docs;
 - b. Insert the image to be used in the email signature into the new document;
 - c. Right-click on the image, select Alt Text, and enter the text that describes the image used or to explain the relation of the image to the associated content; and
 - d. Copy and paste the image from the new document into the signature box in Gmail settings.
4. CDPS email signatures must only include links to information, websites or social media accounts, mottos, taglines or other statements that are directly related to official CDPS business and its mission. Identification of personal pronoun preference is optional.
5. Users must not knowingly:
 - a. Make unauthorized visits to internet sites that could be considered obscene, hateful, offensive, and/or contain other objectionable content or materials;
 - b. Share login credentials, including usernames and passwords, that are used to protect the integrity of all systems;
 - c. Waste work time by playing games, streaming audio or video material, gambling, posting to social networks or newsgroups, or making unauthorized personal purchases or business commitments that are not related to State business;
 - d. Upload or download any computer software programs, applications or patches that are not authorized or performed by OIT;
 - e. Communicate any forms of harassment or intent to harass;
 - f. Create or forward any emails that contain chain letters or Ponzi or other pyramid schemes of any type;
 - g. Send emails soliciting, gambling, or distributing unlawful activities unrelated to CDPS business;
 - h. Send communications containing CJI or CHRI through unsecured media, such as Gmail, Hangouts, or any other medium not compliant with the FBI CJIS Security Policy;
 - i. Store CJI or CHRI within any unsecured database or storage, such as Google Drive or a personally-owned device that is not under



COLORADO

Department of Public Safety

Mobile Device Management of OIT, or other medium not compliant with the FBI CJIS Security Policy.

D. Email Message Retention & Automatic Deletion

1. All emails older than 90 days will automatically be deleted from the system and can not be recovered unless the user retains the email by applying the DONOTDELETE label.
2. Email Trash will automatically permanently remove deleted email 30 days after deletion.
3. Deleted emails within the Trash folder will remain in the Google Vault for 25 days after deletion before being permanently removed from the system.
4. Users may apply the “DONOTDELETE” label to protect an email message from automatic deletion.
 - a. The syntax of the “DONOTDELETE” label must match exactly (all caps and no spaces).
 - b. Users are discouraged from creating sub-labels under the “DONOTDELETE” label because applying only a sub-label will not protect emails from deletion.

VI. REFERENCES

1. Governor’s Office of Information Technology’s Acceptable Use of State Data & IT Resources policy, P-CISP-018
2. State Personnel Board Rule 1-16, 4 CCR 801-1
3. C.R.S. § 24-72-201, et seq. (Colorado Open Records Act - CORA)
4. C.R.S. § 24-72-301, et seq. (Colorado Criminal Justice Records Act - CJRA)
5. CDOT Request Access Form Revised (2019)
6. FBI CJIS Security Policy; version 5.7 (2018)

VII. REVISION HISTORY

1. IT Acceptable Use, Version 1.0, adopted August 16, 2019.
2. IT Acceptable Use, Version 1.1, adopted October 29, 2020.
3. IT Acceptable Use, Version 1.2, adopted May 19, 2021.
4. IT Acceptable Use, Version 1.3, January 17, 2023.