SUPREME COURT OF COLORADO
OFFICE OF THE CHIEF JUSTICE

Directive Concerning the Colorado Judicial Department Electronic Communications Usage Policy: Technical, Security, And System Management Concerns

This directive and attached policy provide direction to the Colorado Judicial Department ("Department") personnel regarding the security, operation and permissible use of the Department's network, hardware and software. In addition, the policy extends to persons who are not Department employees, but use the Department's network, hardware or software with permission of the Department

The policy and procedures contained in the attached Electronic Communications Usage Policy are adopted as an order of the Colorado Supreme Court. This policy shall be entitled "Electronic Communications Usage Policy: Technical, Security, and System Management Concerns," and shall be available to Department personnel and to the public. Department employees shall acknowledge reading the policy and agreeing to follow it.

Done at Denver, Colorado this ___8th____day of September, 2020.

_____/s/_____
Nathan B. Coats, Chief Justice

Colorado Judicial Department

Electronic Communications Usage Policy: Technical, Security, and System Management Concerns

Effective: September 2020
Replaces April 8, 2014 Policy amended June 2018.

Colorado Judicial Department
Electronic Communications Usage Policy:
Technical, Security, and System Management Concerns

1. PURPOSE.

   The purpose of this policy is to provide an electronic communication usage policy for the Colorado Judicial Department ("Department") to protect its information systems from potential threats, vulnerabilities, and data loss, while also describing the responsibilities of the Department's judges and employees (Department users), contractors, volunteers, or business partners.

2. SCOPE.

   This policy applies to all users of Department resources and covers accessing and using the Department's electronic computing technologies, including but not limited to:

   a) The Department's network, which is any circuit used to exchange information within the Department or externally and includes hardware and software necessary to use the network.
   b) Hardware – including but not limited to: desktop computers, laptops, mobile computing devices, remote and centralized servers, network equipment, and telephony equipment.
   c) Software applications – including software developed in-house and purchased commercially.

3. POLICY:

   The security and availability of the Department's information systems and data — in any media or format — is vital to the success of the Department's mission. Therefore, the Department shall establish and maintain a comprehensive Department-wide electronic communication policy detailing acceptable use and behavior necessary to protect the Department's Information Technology (IT) infrastructure, personnel and data assets.

4. INFORMATION SECURITY STANDARDS

   The Department will implement security controls, policies and guidelines to protect information systems and data from individual and environmental threats. Department users accessing the Department network, computing devices or external storage media must make every effort to protect Department information systems and devices within their control.

Department users are responsible for protecting the information technology equipment located within their work areas and any equipment used when working remotely. Department-owned equipment is for authorized use only. Department users are required to implement physical safeguards for all equipment that accesses Department sensitive information and data assets. Equipment must be properly safeguarded and protected to reduce risks from environmental threats and hazards, as well as opportunities for unauthorized access, use, or removal. Such safeguards include, but are not limited to, the following:

a) Electronic communication technologies shall be used for legitimate work-related purposes with limited personal use. Any use of the Department's Case Management System (CMS) must be related to users' performance of their job duties. Any other use is a violation of this policy as well as a violation of the Code of Conduct for employees. The CMS includes: all Department information systems designed to capture, monitor and track court and probation content, including filings, events, calendar events, documents, and financial information in a case; Colorado State Courts – Data Access System; Colorado Courts E-Filing System (CCE); CICJIS; or any other electronic court and probation record-keeping system. Users are strictly prohibited from using the CMS to access information for which they have no legitimate business purposes, including information related to court cases or probation records for individuals with whom a user has a personal relationship, such as spouses or family members, or on individuals who are well known to the public, whether the information is publicly available or not.

b) With the exception of CMS, Colorado State Courts – Data Access System, CCE, CICJIS or any other electronic court and probation record keeping systems, limited personal use of the Department's electronic communication technologies is permissible when it does not consume more than a minimal amount of resources, interfere with employee productivity, conflict with this policy's goals or any other Department policy, or preempt any work-related activity, in accordance with the Colorado Judicial Department Code of Conduct.

c) Department users must utilize strong passwords and have a professional responsibility to protect system passwords by not sharing passwords with anyone. Department users must change passwords per prescribed schedule or immediately if a password is discovered to be compromised. Passwords must always be secured from unauthorized access. Enabling the "Save Password Option" is strictly prohibited.

d) Department users are required to lock their PC, laptop, or mobile computing device when the device is no longer within line of sight. At the end of the

workday, Department users must log off their workstations. The Department will employ access time and system locking procedures to protect against unauthorized use of Department information systems.

e) To the extent possible, computer monitors will be positioned to eliminate viewing by unauthorized personnel. When computer monitors cannot be positioned to eliminate viewing by unauthorized personnel, a privacy screen, which allows viewing only from straight-on, will be used.

f) Department users must ensure any IT related work or maintenance performed on any computing device, system, or network is completed by an authorized ITS employee or contractor of ITS. Express approval from an authorized ITS employee is required prior to removing any computing components and should not be removed without the express approval of ITS. Department users are expected to notify their immediate supervisor of anyone not complying with this procedure.

g) Information technology systems or devices not specifically purchased or authorized by the Department's Chief Information Officer (CIO) are prohibited from being connected to the Department's local and remote network or any other Department information system. This includes, but is not limited to, software applications, all external media (i.e. zip drives, thumb drives, external hard drives, CD burners) and all hardware such as PCs, laptops, mobile computing devices, scanners, printers, and "smart devices."

In situations where there is a business need to connect external media to a computing device or information system, Department users must take precautionary measures to ensure the computing device and information system(s) are properly secured. Precautionary measures shall include, at a minimum, scanning the external media for malware. Business situations that may require connecting unencrypted external media to a computing device or information system may include the following

1) Large exhibits or evidence on external media for court proceedings;
2) Case review for probation supervision purposes; or
3) Training materials that are required to be distributed using external media.

All Department users are expected to comply with Chief Justice Directive 08-03 – Centralized IT Purchasing and Chief Justice Directive 16-03 – Retention, Transmission, and Viewing of Sensitive Records.

h) All Department users who have access to or store Department data must ensure that the data is protected from risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

i) When no longer needed, Department sensitive information must be destroyed by a method rendering it unreadable, undecipherable, and irretrievable.

j) Software Licensing: All software, installed on workstations shall be installed by and registered with ITS. Personally-owned software on any Department information system must be approved by authorized ITS personnel before use. Use of pirated or illegally obtained software on any Department information system is strictly prohibited. To ensure compliance with software copyright and licensing agreements, ITS staff are authorized to conduct computer audits. ITS has the authority to remove or disable any unapproved or pirated software found.

k) All devices that connect to any Department information system, either on site or from a remote location, must be updated with the latest security patches and malware protection as they are distributed. Users will not disable, uninstall or override any security software, settings, or configurations on Department owned equipment.

l) Remote access to the Department's network is permitted only with the use of Multi-Factor authentication and through approved software/services authorized by the Department's CIO.

m) Peer-to-Peer (P2P) software/service connections (where a computer or server acts as a sharing device for users outside the Department's network) are strictly prohibited.

n) A security review must be performed by ITS for any computing device, network, wireless, or server equipment purchased using local district funds, and if approved, installed by authorized ITS personnel.

o) Wireless network installations or configurations needed to access the Department's network must be authorized and performed by ITS. All wireless devices must be approved by authorized ITS personnel before being connected to the network.

p) Portable and/or mobile computing devices regardless of technology or ownership, must meet Department security policies, procedures, and configuration standards.

q) Department users are strictly prohibited from downloading and using any hacking type tools, network scanning software, or password crackers unless specifically approved and authorized by the CIO in writing.

r) All Department users are required to participate in the Department's information security awareness program in accordance with C.R.S. § 24-37.5-404. This training must occur at a minimum once a year. Security

awareness participation will be reflected in the Department's learning management system.

s) All account access will follow the principle of least privilege. The principle of least privilege means granting the minimum access to applications and services which are required to perform a business function

5. SECURITY INCIDENTS

A security incident is a computer, network, or paper based activity that results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data. Security incidents may also include threats, misrepresentations of identity, or harassment of or by individuals using these resources.

All incidents related to information security shall be reported immediately to the user's supervisor and the Information Security team. Colorado Revised Statutes § 6-1-716, requires notification to an individual should a breach of Personal Identifying Information (PII) occur. PII disclosures must follow the directives of C.R.S. § 24-37.5-405.

Department users must immediately report any incident of theft, loss, or compromise of Department sensitive information or information systems to the user's immediate supervisor and the Information Security Manager (ISM).

a) If a compromise of PII has occurred, an appointed incident response team will examine the details surrounding the incident ensuring information and systems are not compromised. If the incident is believed to involve criminal activity, the CIO or ISM will contact local law enforcement.
b) The ISM will track and document information system security incidents on an ongoing basis.
c) Personnel will be provided training by ITS in their incident response roles.

6. UNAUTHORIZED ACCESS

Unauthorized access is defined as not having formal written permission or approval for access to Department systems or data. Unauthorized access to Department information may include access

a) by someone who does not have written Department permission to access the information, or
b) by someone who has met all requirements to access the systems and/or data but accesses the systems and/or data for an unauthorized purpose.

All Department users should be alert to their surroundings and immediately report

any suspicious activity or suspected incidents to their immediate supervisor, the ISM and the CIO.

7. ELECTRONIC MAIL (EMAIL)

Email shall be used for authorized Department purposes. When emails contain sensitive Department data, emails must be appropriately encrypted. Email users must exercise common sense, good judgment, and propriety in using the Department's electronic communication technologies. Department users should not expect privacy or confidentiality when using a Department issued email account and/or Department email system(s). For technical issues or investigative purposes, Department email accounts or system(s) may be subject to review. Such technical issues or investigations include but are not limited to email or email account restoration, troubleshooting email client issues (i.e., Outlook), ITS security investigations, Human Resource investigations, and/or law enforcement investigations. Such reviews will be handled in accordance with appropriate policies and laws. In addition, email may be subject to disclosure as part of a records request pursuant to the Supreme Court rule regarding Public Access to Information and Records (P.A.I.R.R.). Electronic mail messaging shall be used in accordance with the following guidelines:

a) Auto-forwarding of email messages to addresses outside the Department network is strictly prohibited.

b) Misrepresenting, obscuring, or suppressing a user's identity in the "From:" line of an email message or information system is prohibited. The username, email address, organizational affiliation, and related information included with an email message or posting must reflect the actual originator of the message or posting. This does not include deleting information within the body of an email when replying or forwarding information.

c) To ensure the integrity of the Department's email communication system, employees shall not intercept or assist in intercepting email communication unless authorized to do so by the Director of Human Resources or his/her designee in writing and by the CIO.

d) Message Content – All messages shall be conducted in a professional manner and the messaging shall not:

    1) contain profanity, obscenities or derogatory remarks;
    2) contain obscene, pornographic or sexually suggestive materials;
    3) be used to discriminate against any person or group on the basis of race, national origin, gender, age, sexual orientation, religion, socioeconomic status, or disability;
    4) be used to promote religious or political beliefs;
    5) be used to harass and/or threaten others;
    6) be used to intimidate others or to interfere with a person's ability to

perform his or her job duties;

7) involve the creation and exchange of advertisements, solicitations, chain letters or other unsolicited email;
8) involve the creation and exchange of information in violation of any copyright laws; or
9) be used to promote personal and/or self-interests.

e) Care should be taken in opening any email message if the Department user is not familiar with the message sender. If the email message looks suspicious, the Department user should permanently delete the message by pressing "Shift+Delete" And report the message to the ITS security team. If the Department user continues to receive suspicious email from the sender, the local IT Support Technician should be contacted to provide necessary information to the Department's ISM.

f) It is necessary for ITS staff to use software to monitor the activity of user IDs. It may also be necessary for technical support personnel to review the content of an individual employee's communications during the course of problem resolution, or to ensure the ongoing availability and reliability of the email system(s). Under no circumstances, however, may technical support personnel review the content of an individual employee's communications except to enforce provisions of this policy and approved by the Director of Human Resources or his/her designee and the CIO.

1) ITS Security personnel is distinct from technical support personnel and has been authorized by the Department to review the content of an individual employee's communications as necessary and appropriate for purposes of preventing cyber security threats and incidents.

8. ACCEPTABLE USAGE POLICY

All Department users who require or need to establish access to Department information systems must read, understand and agree by signature to adhere to the Department's Acceptable Usage Policy (Attachment A).

The Department has established a set of rules that describe the responsibilities and expected behavior regarding information system usage. These rules clearly delineate security responsibilities and expected behavior of all system owners and Department users. The rules include the consequences of inconsistent behavior or non-compliance when using Department information systems. All Department users will have access and/or a copy of the Acceptable Usage Policy for review. A signed acknowledgement of this policy is a condition of access to any Department information system.

9. IMPLEMENTING THIS DIRECTIVE

ITS will implement the provisions of this directive using various security controls

including but not limited to malware detection/prevention programs, intrusion detection software, internet blocking programs, encryption practices, firewalls, and methodologies for centrally distributing critical security updates from approved Department software or hardware providers.

Colorado Judicial Department
Acceptable Usage Policy

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, Department information, including sensitive information such as PII or information systems of the Colorado Judicial Department.

GENERAL ACCEPTABLE USAGE POLICIES AND PROCEDURES

a. I understand that when I use any Department information system, I have NO expectation of privacy in any Department records that I create or in my activities while accessing or using the Department's information systems.
b. I understand that the Administrative Authority, with the approval of the Director of Human Resources or his/her designee and the Chief Information Officer, may review my conduct or actions concerning Department information and information systems, and take appropriate action if warranted.
c. I understand under no circumstances may I use the Department's Case Management System, Colorado State Courts – Data Access System, Colorado Courts E-Filing System (CCE), CICJIS or any other electronic court and probation record keeping system for personal or non-work related purposes.
d. I understand that I am allowed limited personal use of the Department's electronic information systems if it does not consume more than a minimal amount of resources, does not interfere with employee productivity, does not conflict with the goals of CDJ 07-01, or preempt any work related activity, in accordance with the Colorado Judicial Department Code of Conduct.
e. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, unauthorized deleting of information on Department systems, or unauthorized denying or granting access to Department systems; modifying Department systems; using Department resources for unauthorized use on Department systems, or otherwise misusing Department systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.
f. I understand that I have a responsibility to report suspected or identified information security incidents to the Information Security Team, Information Security Manager (ISM), or my supervisor as appropriate.
g. **I understand that if I refuse to sign this Acceptable Usage Policy as required by Department policy, I will be denied access to Department information and information systems. Any refusal to sign the Department's Acceptable Usage Policy may have an adverse impact on my employment with the Department.**

SPECIFIC ACCEPTABLE USAGE POLICIES AND PROCEDURES

a. I will follow established procedures for requesting access to any Department computer system and for notification to appropriate Department personnel when access is no longer needed. Such notification will include my immediate supervisor and/or Administrative Authority and ITS.
b. I will follow established Department information security policies and procedures.
c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware public domain, or open source.
d. I will not attempt to override, circumvent or disable operational, technical, or security controls put in place unless expressly directed to do so in writing by the Department's CIO.
e. I will follow the principle of least privilege with my user account and appropriately use any administrative accounts I may be provided.
f. I will protect my passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the Department's minimum password requirements.
g. I will ensure that I log off or lock any computer, console, or mobile computing device before walking away and will not allow another user to access any computer, console, or mobile computing device while I am logged on to it other than for troubleshooting purposes performed by ITS.
h. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any Department electronic communication system.
i. I will not attempt to probe computer systems to exploit system controls or access Department sensitive data for any reason other than in the performance of official job duties.
j. I will protect Department property from theft, loss, destruction, or misuse. I will follow Department policies and procedures for handling IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for Department activities.
k. I will never swap or surrender Department hard drives or other storage devices to anyone other than an authorized ITS employee at the time of system problems.
l. I will not disable or uninstall software programs used by the Department that auto-installs security software updates to Department computer equipment.
m. I agree to allow authorized ITS or Human Resource personnel to examine — for trouble shooting or disciplinary purposes — any Department or personal IT device that I have been granted permission to use, whether remotely or in any setting to access Department information for purposes of creating, storing or using Department information.
n. I agree to have all equipment scanned by authorized ITS staff prior to connecting to the Department network if the equipment has not been connected to the Department network for a period of more than three weeks. I agree to adhere to Department ITS guidance on maintaining Department issued devices and keep them appropriately

patched and updated.

o. I will complete mandatory periodic security awareness training within designated time frames and complete any additional required training for the systems to which I require access.
p. I agree that I will not allow Department sensitive information or data to reside on non- Department systems or devices unless specifically designated and approved in advance by the Department's CIO. I agree that I will not access, transmit or store remotely any Department sensitive information that is not properly encrypted.
q. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction.
r. I will use Department-provided encryption to encrypt any e-mail, including attachments to the email, which contains Department sensitive information before sending the e-mail. I will not send any email that contains Department sensitive information in an unencrypted form. Department sensitive information includes Personally Identifiable Information (PII) and protected health information.
s. I will immediately inform my supervisor if I lose control over any portable device that contains sensitive information, encrypted or unencrypted. Immediately means as soon as the loss is noticed; not more than one hour after the loss is noticed. Notice should be made by email and a telephone call.

3. Acknowledgement and Acceptance

a. I acknowledge that I have received a copy of the Department's Acceptable Usage Policy.
b. I understand, accept and agree to comply with all terms and conditions of this Acceptable Usage Policy.

_____ _____

[Print or type your full name] Signature

_____ _____

Date Office Phone