



CANYON COUNTY COMMISSIONERS

Leslie Van Beek
District I

Brad Holton
District II

Zach Brooks
District III

Greg Rast, Chief Operating Officer

1115 Albany ❖ Caldwell, Idaho 83605 ❖ Telephone: (208) 454-7507 ❖ Fax: (208) 454-7336

MOBILE DEVICE AND REMOTE ACCESS POLICY (STIPEND REMOVAL / MFA)



Table of Contents

MOBILE AND REMOTE ACCESS OVERVIEW	2
CANYON COUNTY POLICY REGARDING ASSIGNMENT OF MOBILE DEVICES.....	2
CANYON COUNTY POLICY REGARDING REMOTE ACCESS	3
AUTHORIZATION.....	4
USER RESPONSIBILITIES	4
TERMINATION OF ACCESS.....	5
EXHIBIT A – MOBILE DEVICE AND REMOTE ACCESS AUTHORIZATION FORM	7

MOBILE AND REMOTE ACCESS OVERVIEW

Definitions:

- Canyon County: the political subdivision and employer, hereinafter referred to as “County”.
- COD - “County Owned Devices” includes but not limited to smartphones, tablets, laptops, computer workstations and cellular devices. All CODs shall be asset tagged.
- POD - “Personally Owned Devices” includes but not limited to smartphones, tablets, laptops, computer workstations and cellular devices.
- Users - authorized individuals who can access County network resources via a COD outside of the Canyon County network.
- Jail breaking - Operating System (OS) modification meant to modify the original operating system in a way that allows the user of the device to bypass standard built-in security features and controls. Routine changes in settings and the device’s applications do not constitute OS modification.
- MFA – “Multi-Factor Authentication” is defined as a security measure that requires Users to provide two or more verification factors to access internal systems. MFA may be secured through either a mobile application or a FOB provided by the County to Users.
 - Fob - Secure Token Fobs are used for MFA purposes. This device is also known as a random number generator displaying a unique number every 30 seconds.
- MDM – “Mobile Device Management” is an enterprise software platform to manage and secure mobile iPhone Operating System (IOS) equipment.
- CCIT – “Canyon County Information Technology” services and personnel.

CANYON COUNTY POLICY REGARDING ASSIGNMENT OF MOBILE DEVICES

Protecting unlawful access by and through mobile devices and equipment being used off County property and allowing secured remote access with encryption that safeguards public data is an important part of County business and security. Canyon County hereby adopts the following mobile device and remote access policy requirements:

1. POD equipment is not approved or supported to conduct County business in any capacity. Under this policy, employee stipends will no longer be approved for the use of previously approved POD

equipment. All employees must use COD devices to remotely access and conduct County business.

2. MFA services combined with the use of COD equipment for remote access is mandatory.
3. CCIT will ensure all CODs are configured, tested, protected and set hardware requirements for a positive and secure end-user experience.
4. All Users must use CODs to conduct County business, and those CODs will be managed by CCIT to push security updates while utilizing current endpoint protection software.
5. Multi-factor authentication can be used either by Fob or by assigned COD with an authorized mobile app. Pre-approval of COD, Fob and/or remote access is required by authorized management of the associated office or department. The approvals are done on an individual User basis but must be done with approved COD devices.

CANYON COUNTY POLICY REGARDING REMOTE ACCESS

Remote access allows continued productivity outside of the Canyon County network. In most cases, remote access originates from networks that are out of the County's control and/or are at locations where the internet connection is at a lower security posture.

The purpose of this authorization is to set expectations for remote access by Users from any external location. These User and COD requirements are designed to minimize the potential risk exposure as a result from the use of remote access. Risk damages include the loss of sensitive information, security breaches, ransomware, malicious malware, virus infections or corruption of critical Canyon County internal systems. **Remote Access is for employee work purposes only.** Accessing County webmail is an exception to this rule and can be accessed outside of the County network on any public internet connection through a preferred web browser and does not require remote access.

The County has adopted a standard using enterprise Apple IOS devices using an MDM solution to perform two primary functions: (1) ensure that mobile devices are properly protected by having proper security including: passwords, software protection and have screen locks in place and, (2) allow CCIT to recover County locked devices, disable mobile access or remote wipe devices when necessary. **Android** devices are not supported or managed under this policy. Remote access has the following two options available for a secure connection.

1. A COD can be procured through CCIT and charged to the associated office or department to conduct County business with the use of multi-factor authentication, email and full mailbox sync, phone, text or any other assigned use by the elected official or department administrator.
2. A COD or a Fob can be assigned for MFA remote services; This device is allocated from CCIT and not charged back to the associated budget.
 - a. Secure token fobs will also be assigned to County employees that do not have a COD with the DUO security application installed. This is needed in order to log into your computer(s) and associated Microsoft Office 365 accounts. These will be issued along with your identification badge.

The Canyon County Sheriff's Office Emergency Technical Services (ETS) work in conjunction with CCIT for issuing COD equipment, which aligns with this policy. The exception to this policy is COD equipment used for the purposes of 911 services, dispatch, public safety systems or emergency response.

AUTHORIZATION

Canyon County requires an authorization form (Exhibit A) approving COD and secure token fobs and/or remote access for any User with the full understanding of this policy and expectations. CCIT will not enable remote access fobs or COD devices without proper authorization.

USER RESPONSIBILITIES

Responsibilities:

- Users shall take proper care of COD and/or fobs to protect from theft, damage, abuse, and unauthorized use.
- Users must maintain the COD as provisioned and received, keep the device current with security patches and updates, and not engage in jail breaking of the device. Users are to not alter or disable security features on the COD. A violation of tampering or disabling security will lead to revocation of the device and lead to disciplinary actions.
- Users must keep assigned Fob with them during their work shift.
- All CODs will be managed by the CCIT department through an authorized MDM platform where the devices can be secured and recovered.

- Users who wish to access County network resources using approved COD equipment must password-protect the device. The password must be a minimum 4-digit passcode or the use of biometrics. The Canyon County email system will ensure that a qualifying password is set in place upon activation of the COD for email mailbox synchronization.
- International cell coverage will be evaluated on a case-by-case basis and must be pre-approved.
- It is the responsibility of the user to ensure their home networking equipment and internet connection is set up correctly and enough bandwidth to allow remote access connections to the County. CODs will come preloaded with end-user protection software and the necessary connection agents.
- Within 10 days of written notification from the County, the user may also be required to reimburse the County if the user's COD is lost, stolen, damaged, or destroyed because of negligence, improper use, or willful action on the employee's part.
 - Determination of whether reimbursement is required is at the discretion of the users' elected official or department administrator.
- If a COD is lost or stolen, the user must notify their elected official or department administrator, as well as the County IT Help Desk by calling (208) 454-7300 or emailing helpdesk@canyoncounty.id.gov within one hour, or as soon as practical after the user notices the device is missing.
 - CCIT may lock and disable the device upon notification, wipe the device and disable County email access from the device.
- There is no expectation of privacy of a COD.

TERMINATION OF ACCESS

The County reserves the right to revoke a COD or Fob for any reason, including but not limited to non-use, limited business use, excessive personal use, budget restrictions, or changes to this policy.



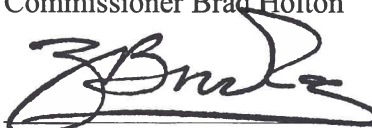
Upon voluntary employee resignation, COD devices and fobs will be required to be turned into the associated office or department at the time of departure. All files and data on the device shall be made available and any passwords provided. The COD device shall be delivered to CCIT to perform a remote or in-person wipe "erase" to set the device back to factory default.

Upon involuntary employee termination, under any circumstances, CCIT will be notified by the elected official, department administrator or designee to perform a COD remote wipe "erase" to set the device back to factory default, or at a minimum, disable email synchronization to the device. Fobs will be deactivated and recovered with the County issued identification badge. The COD will be collected to either hold for litigation, repurposed for County business or go through the equipment end-of-use process either by disposal, donation or public auction.

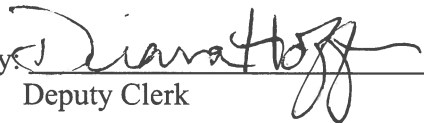
DATED this 3rd day of October, 2025.

BOARD OF COUNTY COMMISSIONERS

X Motion Carried Unanimously
 Motion Carried/Split Vote Below
 Motion Defeated/Split Vote Below

	Yes	No	Did Not Vote
 _____ Commissioner Leslie Van Beek	<u>✓</u>	<u> </u>	<u> </u>
 _____ Commissioner Brad Holton	<u>X</u>	<u> </u>	<u> </u>
 _____ Commissioner Zach Brooks	<u>X</u>	<u> </u>	<u> </u>

ATTEST: RICK HOGABOAM, CLERK

By: 

Deputy Clerk

EXHIBIT A – MOBILE DEVICE AND REMOTE ACCESS AUTHORIZATION FORM

Reference Mobile and Remote Access policy guidelines.

USE: (Select all that applies)

- Remote access Authorization ☐
- Secure Token Fob ☐
- COD Authorization ☐
- County Equipment ☐

SN: _____

Cell Number: _____

Identified Equipment:

I HAVE READ THE POLICY AND WILL ADHERE TO THE GUIDELINES AND RULES ASSOCIATED TO MOBILE AND/OR REMOTE ACCESS TO PERFORM THE DUTIES OF MY POSITION.

Employee (Print): _____

Employee Signature: _____

Office/Department: _____

I AUTHORIZE THE FOLLOWING ACCESS:

Elected Official / Department Administrator / Designee

Print Name

Signature