

DILWORTH POLICE DEPARTMENT

PORTABLE VIDEO AUDIT

Submitted by Haider Howitzer, LASO

The Mobile Video Recorder audit (body cams) was performed by Haider Howitzer on 4/23/2025 with the assistance of Stacy Pritchard, TAC and Program Administrator with the Dilworth Police Department. We conducted an audit of the following policies and procedures used for handling the body cam video data.

1. Policy Manual
2. Cameras and equipment used
3. Record storage and classification
4. Retention policies
5. Data user security
6. Data sharing with other agencies

Mobile Video Recorders Policy (Appendix A)

A policy manual is assembled by the Dilworth Police Department which details procedures for the maintenance and usage of the body cam equipment.

Cameras and Equipment (Appendix B)

The Dilworth Police Department's inventory of portable video equipment includes nine (9) Axon Body 3 cameras, eight (8) Axon Body 2 cameras and two (2) docking stations. One docking station and the eight (8) Axon Body 2 cameras are no longer in use. All cameras are assigned to individual officers so as to ensure proper data assignment and maintain a strict data evidence chain of command.

Record Storage and Classification (Appendix C)

All MVR data is uploaded to Evidence.com. The data is housed on external servers that are hosted and managed by Axon Enterprises. This storage is a secure site with a multi-level identification system and can only be accessed with individual credentials. Each video is stored with its own ID including a time and date stamp embedded into the data. Each data piece is also tagged by case number and categorized by officers.

Retention Policies (Appendix D)

Every video is set with a pre-determined retention schedule that is selected by the agency administration. The Dilworth Police Department uses the State of MN Data Retention Policies. Automatic deletions of data are set within these policies. Only authorized agency administrators have the capability of manually deleting any data.

Data User Security Risk (Appendix E)

All officers are assigned to a "Patrol Basic" role. This allows for limited access to patrol officers. The "Basic" role allows for "view only" rights as well as categorizing and labeling videos that were recorded by each officer. Currently, there are only two individuals assigned as an "Admin Pro" role - Chief Hunter Rawson and TAC Stacy Pritchard. All videos contain a complete audit trail automatically recorded by the Axon system to ensure security and identify any access issues.

Data Sharing with Other Agencies (Appendix F)

The Dilworth Police Department currently has four partner agencies for data sharing purposes, the Clay County Attorney's Office, the City of Moorhead Attorney's Office, Glyndon Police Department and Barnesville Police Department. As partner agencies, they are given a login through Axon to access Evidence.com. However, they are only given permission to view specific videos assigned on a case-by-case basis. They are sent an automated email for downloading individual case videos.

Conclusion

The Dilworth Police Department's policies and procedures for mobile video recording are in compliance with MN Statute 13.825 for Portable Recording Systems.

Respectfully submitted,

Haider Howitzer, LASO
330 34th Ave E, Unit2
West Fargo, ND 58078
haider@howitzer.io
701-541-5494

Appendix A

Mobile Video Recorder Policy

MOBILE VIDEO RECORDERS POLICY

I. POLICY

A. To establish uniformed guidelines for the operation of Mobile Video Recorders (MVR), and to establish a schedule for the retention of the video evidence. The primary use of MVR for the Dilworth Police Department is for the purpose of collecting evidence to be used in the prosecution of persons who violate the law and to provide objective information concerning police/citizen contacts in accordance with law.

II. SCOPE

This policy governs the use of MVRs in the course of official duties. It does not apply to the use of surreptitious recording devices in undercover operations or the use of squad-based (dash-cam) video recorders. The chief or chief's designee may supersede this policy by providing specific instructions for the use of MVRs to individual officers, or providing specific instructions for the use of MVRs pertaining to certain events or classes of events, including but not limited to political rallies and demonstrations. The chief or chief's designee may also provide specific instructions or standard operating procedures for MVR use to officers assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities.

III. DEFINITIONS

- A.** Mobile Video Recorder MVR – A camera worn on an individual officer's person that records and stores audio and video.
- B.** Program Administrator – Person identified by the Chief of Police to administer the storage, retention of video evidence.
- C.** Digital Evidence – MVR files, including photographs, audio recordings and video footage captured by a MVR, all metadata stored digitally.
- D.** Metadata – Case numbers, Incident numbers (ICR) and other descriptors used to identify digital evidence.

IV. PROCEDURES

A. Officer Safety takes Precedence over Recording an Event

1. Officers shall follow existing officer safety policies when conducting enforcement stops as outlined in departmental policies and procedures. Officer safety shall be the primary consideration when conducting official law enforcement duties and facilitating police/citizen contacts.

B. General

1. Enhance Officer Safety.
2. Enhance Public Trust.
3. Only authorized personnel shall use or be in possession of a MVR device.
4. MVR equipment is for official use only and shall not be utilized for personal use.
5. Allow for accurate documentation of police-public contacts, arrests and critical incidents. They also serve to enhance the accuracy of officer's reports and testimony in court.
6. Enhance this agency's (Dilworth Police Department) ability to review probable cause arrest, officer and suspect interaction and evidence for investigative and prosecutorial purposes and to provide additional information for officer evaluation and training.
7. Officers shall not tamper with or dismantle any hardware or software component of any "MVR" device.
8. The use of any other personal recording device for the same purpose is not authorized without written permission of the Chief of Police.
9. All digital evidence collected using the MVR is considered a record of the Dilworth Police Department and is for official use only.
10. Accessing, copying, forwarding or releasing any digital evidence for other than official law enforcement use and contrary to this procedure is strictly prohibited. Public release of digital evidence is prohibited unless approved by the Chief of Police.
11. Personal computer equipment and software programs shall not be utilized when making copies of digital evidence. Using a secondary recording device such as a video camera, cell phone or other device to record or capture digital evidence from DPD servers is strictly prohibited.
12. Officers shall not intentionally edit, alter, or erase any MVR recording unless otherwise expressly authorized by the chief or the chief's designee.

C. Pre-Shift Inspection

1. Officers shall inspect their assigned MVR devices daily to ensure there is no visual damage and the device is in working order.
2. Visual damage shall be immediately documented by contacting a supervisor either on shift or by email.
3. Inoperable equipment shall be presented to the MVR Equipment Officer or to on duty supervisor.

D. Camera Position

1. Officers shall wear their assigned MVR on their uniform so that it captures the events as they happen.
2. It shall be the responsibility of the officer due to differences in stature of officers, to adjust the MVR appropriately to capture all desired video.
3. Officer's failure to appropriately adjust MVR while being worn is not acceptable and a violation of department policy.

E. Advisements about Recordings

1. Private Citizens do not have a reasonable expectation of privacy when talking with police officers during the scope of an officer's official duties, even when the contact is in a private residence. Therefore, officers are not required to give notice they are recording. However, if asked, officers shall advise citizens they are being recorded.
2. Officers are not to initiate or cease recording an event, situation or circumstance solely at the demand of a citizen.
3. Officers and supervisors involved in the investigation of a complaint against a member of the police department must inform complainants and witnesses they are being recorded.
4. Officers shall not intentionally block the MVRs audio or visual recording functionality to defeat the purposes of this policy.

F. When and Where to Record

1. Police personnel who are assigned MVR must complete an agency approved and/or provided training program to ensure proper use and operations. Additional training may be required at periodic intervals to ensure the continued effective use and operation of the equipment, proper calibration and performance and to incorporate changes, updates or other revisions in policy and equipment.
2. Enforcement Related Contacts
 - a. Officers shall use the event mode to record enforcement related contacts. The event mode should be activated prior to actual contact with the citizen, or as soon as safely possible thereafter, and continue recording until the contact is concluded.
 - b. Enforcement related contacts may include but not be limited to the following: Traffic stops, filed interviews, detentions, arrests, persons present at radio calls who are accused of crimes, and consensual encounters in which the officer is attempting to develop reasonable suspicion on the subject of the encounter.
 - c. Covering another City employee or law enforcement officer during an enforcement contact.
 - d. Officer working plain clothes assignments are exempt from this policy.
3. Arrests
 - a. Officers may stop recording when the arrestee is secured inside a police car or law enforcement facility. If an arrestee becomes uncooperative, or if there is some evidentiary purpose, officers should resume recording.
 - b. If the officer resumes recording, the camera shall remain on until the officer no longer has contact with the subject.
4. Suspect Interviews
 - a. Officers are encouraged to fully record suspect interviews. Officers should not stop and start the recording during suspect interviews.
 - b. When recording interviews, officers shall ensure they record and admonishments (Miranda Warning – when appropriate) prior to the start of the interview.

5. Private Residences

a. Private Citizens have a reasonable expectation of privacy in their homes. However, when officers are lawfully present in a home in the course of official duties, there is no reasonable expectation of privacy.

6. Searches

a. During the execution of a search warrant, an arrest warrant, a Fourth Amendment waiver search, or a consent search in which the officer is looking for evidence or contraband.

G. When and Where Not to Record

1. Communication with other police personnel without the permission of the Chief law Enforcement Officer (CLEO)

2. Encounters with undercover officers or confidential informants

3. "MVR" shall not be used to record non-work related activity

4. "MVR" shall not be used to record in areas or activities such as pre-shift conferences, department meetings, locker rooms, break rooms, or other activities not related to a criminal investigation

5. "MVR" shall not be used during department administrative investigations

6. General interactions with (for example but not limited to co-workers, supervisors, Chief of Police, City Administrator, Mayor and Council Members or any other employees of the City of Dilworth.

7. Patient Privacy

a. Officers shall not record patients during medical or psychological evaluations by a clinician or similar professional or during treatment, unless required for evidentiary purposes (e.g. Legal Blood Draw). Officers shall be aware of patients' rights to privacy when in hospital settings. When recording in hospitals and other medical facilities, officers shall be careful to avoid recording persons other than the suspect.

b. Officers shall not record while in a facility whose primary purpose is to provide psychiatric services unless lawfully present in the course of official duties responding to a radio call involving a suspect who is still present.

c. Officers shall not record while inside jail facilities.

8. Generally, officers should not record informal or casual encounters with members of the public. Officers should consider that recording people in some circumstances may inhibit sharing neighborhood information or developing strong ties between members of the community and officers.

9. Officers are not authorized to use any type of personal recording device.

H. Surreptitious Recordings

Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Minn. Stat. § 626A.02).

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation. Members shall not surreptitiously record another

department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee

I. Documentation of MVR Use and Nonuse

1. Whenever an officer makes a recording, the existence of the recording shall be documented on ICR's, Arrest reports, and related reports and as appropriate.
2. Whenever an officer fails to record an activity required to be recorded under this policy or captures only a part of the activity, the officer must document the circumstances and reasons for not recording on ICR's, Arrest reports, other related reports and as appropriate. Supervisors shall review these reports and initiate any corrective action deemed necessary.

K. Entering Metadata

1. Each recorded segment requires metadata be entered, even if the segments are of the same event. Metadata should be added at the conclusion of the event. In case of a delay, metadata should be added as soon as possible but no later than the end of the officer's scheduled shift.

L. Downloading Procedure

1. Officers are responsible for downloading their MVR at the end of each shift and adding metadata. Officers shall place the MVR into the docking station; this will allow the data to be transferred from the MVR through the docking station to Evidence.com. The data is considered impounded at this point and the MVR is cleared of existing data. The MVR should not be removed from the docking station until the data has been uploaded and the battery fully charged. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's MVR and assume responsibility for transferring the data from it.

M. Accessing Downloaded Digital Evidence

1. All Officers are responsible for accessing their own digital evidence, Officers are not authorized to copy, change or delete any MVR for other Officers.
2. Peace officers shall observe the confidentiality of information available to them due to their status as peace officers.

L. Retention of Digital Evidence

1. Digital Evidence is securely stored in accordance with the Minnesota Government Data Practices Act and the Minnesota State Records Retention Laws and no longer useful for purposes of training or for uses in an investigation or prosecution. In capital punishment prosecutions, recording shall be kept permanently. Listed below is a guideline for retention of video types not all inclusive.

Uncategorized 90 Days
Case File 7 years
Miscellaneous 90 Days
Pending Review Manually
Permanent Case File Manually
Traffic Citations 3 years
Training Exercises Manually
Internal Investigations Manually

N. Reviewing Downloaded Digital Evidence

1. Officers may review their own recordings.
2. The Dilworth Police Department Investigator is responsible for reviewing, updating and tracking digital evidence associated with assigned cases.
3. Digital evidence captured by the MVR is not all inclusive. The system captures a less broad and less detailed image than the totality of the human senses. An officer's recollection of specific details may be different than what is captured in digital evidence. Officers should review digital evidence prior to completing reports when necessary to ensure accuracy. Officers shall review digital evidence prior to providing testimony at hearings, trial or depositions.
4. It is not the intent of the Department to review digital evidence for the purpose of general performance review, for routine preparation of performance reports or to discover policy violations.
5. Digital Evidence may be viewed for administrative purposes to include but not limited to
 - a. Any incident in which a member of the Dilworth Police Department is injured or killed during the performance of their duties.
 - b. Any incident involving the use of force by a member of the Department which results in injury or death.
 - c. Any in-custody death.
 - d. Any police pursuit.
 - e. When any member of the Department intentionally or unintentionally discharges a firearm at a person regardless whether an individual is struck.
 - f. When any member of the Department not involved in training intentionally or unintentionally discharges a "Conductive Energy Weapon" at a person including the application of a drive stun.
 - g. Officer involved traffic collision.
 - h. Prior to release of recording in response to proper legal request (Ex: subpoena or other court order).
 - i. In preparation for a civil deposition or responding to an interrogatory where the incident arises from the employee's official duties.

j. When preparing to testify in a criminal, civil or administrative proceeding arising from the employee's official duties.

k. For investigations undertaken by the Dilworth Police Department, for the purpose of providing or disproving specific allegations of misconduct.

l. For administrative proceedings, when digital evidence is used by the Department for the purpose of proving or disproving allegations of misconduct, only digital evidence relevant to the investigative scope shall be viewed and retained by investigators. Information relevant to the recordings viewed and seized as evidence by investigators shall be documented as part of the chronological summary of any investigation undertaken by the Department.

m. At least on a monthly basis, supervisors will randomly review MVR recordings to ensure that the equipment is operating properly and that officers are using the devices appropriately and in accordance with policy and to identify any area in which additional training or guidance is required.

6. In situations where there is a need to review digital evidence not covered by this procedure, the Chief Law Enforcement Officer or his designee must approve the request. Each situation will be evaluated on a case by case basis.

O. Discovery of Inappropriate or Improper Conduct

1. Supervisors reviewing event recordings should remain focused on the incident or incidents in question and review only those recordings relevant to their investigative scope. If inappropriate or improper conduct is discovered during any review of digital evidence, the Supervisor may take the necessary steps to counsel, train or recommend for discipline the officer involved, in adherence with local department policy and/or current union bargaining agreement.

P. Copying and Releasing Digital Evidence

1. Digital evidence captured by "MVR" shall be treated as official records and handled pursuant to existing Department policies, procedures, and state law.

Q. Use of Digital Evidence for Training Purposes

1. Officers and supervisors may find it useful and are encouraged to review recordings of incidents of which they were involved when beneficial for the purpose of conducting a tactical debrief. When an incident is recorded which may be of value as a training aid for a broad section of the Department, the recording officer or that officer's supervisor should contact the Chief Law Enforcement Officer (CLEO) who will review the digital evidence to determine the value of the incident for training. If the CLEO determines the incident would be an appropriate training aid, the CLEO shall obtain approval from the Department Legal Advisor.

R. MVR Program Administrator Responsibilities

1. MVR Program Administrators shall be the Chief of Police or his designee of the Dilworth Police Department. MVR Program Administrators are responsible for performing the following duties.

- a. Maintain and troubleshoot the MVR units
- b. Maintain a record assigned MVR and related equipment
- c. Be proactive and able to complete minor repairs
- d. Arrange for the warranty and Non-warranty repair of the MVR unit
- e. Repair or replace MVR components (Camera, leads, charging units etc.)
- f. Maintain MVR equipment repair and maintenance records
- g. Update software and system settings as necessary
- h. Train officers on current policy and proper use of "MVR" units

Rev 04/17

Appendix B

Cameras and Equipment

BODY CAMERA SEARCH

SERIAL NUMBER

DEVICE NAME

ASSIGNED TO

UPLOAD DATE

Start

End

SHOW ADVANCED SEARCH

RESET FILTERS

SEARCH

Body Worn Cameras

UPDATE STATUS

UPDATE NAME

EXPORT

18 results | 18 selected

<input checked="" type="checkbox"/>	Model	Ser...	De...	Assig...	La... ↓	De... ↑	Err...	Fir...	Wa...	Last D...	Camer...	Maint...	
<input checked="" type="checkbox"/>	Axon B...	X60A56...	X60A56...	STET	Mar 31, ...	Assigned	Good	1.2504.1	None	Mar 31, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A58...	X60A58...	McCl	Mar 31, ...	Assigned	Good	1.2504.1	None	Mar 31, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A59...	X60A59...	Monr	Mar 30, ...	Assigned	Good	1.2504.1	None	Mar 31, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A59...	X60A59...	Hove	Mar 28, ...	Assigned	Good	1.2504.1	None	Mar 31, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A58...	X60A58...	Dann	Mar 28, ...	Assigned	Good	1.2504.1	None	Mar 31, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A55...	X60A55...	Page	Mar 26, ...	Assigned	Good	1.2504.1	None	Mar 31, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A54...	X60A54...	Mitcl	Mar 25, ...	Assigned	Good	1.2504.1	None	Mar 31, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A58...	X60A58...	Raws	Mar 25, ...	Assigned	Good	1.36.47	None	Mar 25, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	X60A53...	X60A53...	Sharj	Dec 30, ...	Assigned	Good	1.24.18	None	Mar 28, ...	Docked		
<input checked="" type="checkbox"/>	Axon B...	x81011...	X81011...	Unassig...	Apr 21, ...	Scrapped	None	1.26.1	Nov 2, 2...	None	None		
<input checked="" type="checkbox"/>	Axon B...	x81019...	X81019...	Unassig...	Apr 21, ...	Scrapped	None	1.26.1	None	None	None		
<input checked="" type="checkbox"/>	Axon B...	x81005...	X81005...	Unassig...	Apr 20, ...	Scrapped	None	1.26.1	None	None	None		
<input checked="" type="checkbox"/>	Axon B...	x81016...	X81016...	Unassig...	Apr 20, ...	Scrapped	None	1.26.1	None	None	None		
<input checked="" type="checkbox"/>	Axon B...	X81184...	X81184...	Unassig...	Apr 20, ...	Scrapped	None	1.26.1	Nov 19, ...	None	None		
<input checked="" type="checkbox"/>	Axon B...	x81018...	X81018...	Unassig...	Apr 16, ...	Scrapped	None	1.26.1	None	None	None		
<input checked="" type="checkbox"/>	Axon B...	x81012...	X81012...	Unassig...	Jan 16, ...	Scrapped	None	1.26.1	Nov 2, 2...	None	None		

<input checked="" type="checkbox"/>	Model	Ser...	De...	Assig...	La... ↓	De... ↑	Err...	Fir...	Wa...	Last D...	Camer...	Maint...
<input checked="" type="checkbox"/>	Axon B...	x81018...	X81018...	Unassig...	Jun 8, 2...	Scrapped	None	1.25.16	None	None	None	
<input checked="" type="checkbox"/>	Axon B...	x81019...	X81019...	Unassig...	Jul 11, ...	Relinqui...	None	1.17.106	None	None	None	

100 per page ▾ 1—18 of 18 items

< 1 >

Appendix C

Record Storage and Classification

EVIDENCE	CASES	RESPOND	ALPR	INVENTORY	REPORTS	ADMIN	19	MY ACCOUNT Last login Mar 31, 2025 SIGN OUT
AGENCY PROFILE	PARTNER AGENCIES	RETENTION CATEGORIES	FIELD VALIDATION	EVIDENCE PLAYBACK SETTINGS				
ROLES & PERMISSIONS	USER-BASED LICENSES	RANKS	COMMUNITY REQUEST SETTINGS	DEVICE HOME				
REDACTION SETTINGS	CASE SETTINGS	ALPR SETTINGS	ALPR POLICY AND USAGE					






Roles & Permissions

License limits


PRO LICENSES	2	BASIC LICENSES	16	A LA CARTE STORAGE	2220 GB	UNLIMITED STORAGE	?
0	remaining	9	remaining	-1922.4 GB	remaining	772.4 GB	used
2	used	7	used	4142.4 GB	used		

[CREATE ROLE](#)
[ASSIGN ROLES](#)


Pro Roles

Role Name	Users In Role	Date Created	Actions
Admin	2	04/26/2016	
Armorer	0	04/26/2016	
Investigator	0	04/26/2016	
New User	0	06/10/2019	
User	0	04/26/2016	

Basic Roles

Role Name	Users In Role	Date Created	Actions
Patrol	7	11/02/2020	

Lite Roles

Role Name	Users In Role	Date Created	Actions
Assignee Only	0	04/26/2016	

Lite Armorer

0

02/28/2017



Lite User

0

02/28/2017



© 2025 Axon Enterprise, Inc. All rights reserved. [Privacy Policy](#). v2025-03-25.206860 Axon Evidence March 2025 CHROME 134.

Appendix D

Retention Policies

EVIDENCE

CASES

RESPOND

ALPR

INVENTORY

REPORTS

ADMIN

19

MY ACCOUNT

Logout Mar 31, 2025

SIGN OUT

AGENCY PROFILE

PARTNER AGENCIES

RETENTION CATEGORIES

FIELD VALIDATION

EVIDENCE PLAYBACK SETTINGS

ROLES & PERMISSIONS

USER-BASED LICENSES

RANKS

COMMUNITY REQUEST SETTINGS

DEVICE HOME

REDACTION SETTINGS

CASE SETTINGS

ALPR SETTINGS

ALPR POLICY AND USAGE

Retention Categories

ADD CATEGORY

NAME	RETENTION DURATION	CATEGORY RESTRICTIONS	
Uncategorized	90 days		
CASE FILE	7 years	Unrestricted	
Miscellaneous	90 days	Unrestricted	
Pending Review	Until manually deleted	Unrestricted	
Permanent Case File	Until manually deleted	Unrestricted	
Traffic Citations	3 years	Unrestricted	
Training Demo	Until manually deleted	Unrestricted	
Use of Force / IA	Until manually deleted	Unrestricted	

Appendix E

Data User Security

EVIDENCE

CASES

RESPOND

ALPR

INVENTORY

REPORTS

ADMIN

19

MY ACCOUNT
Last login Mar 31, 2025
SIGN OUT

AGENCY PROFILE

PARTNER AGENCIES

RETENTION CATEGORIES

FIELD VALIDATION

EVIDENCE PLAYBACK SETTINGS

ROLES & PERMISSIONS

USER BASED LICENSES

DARKS

COMMUNITY REQUEST SETTINGS

DEVICE HOME

REDACTION SETTINGS

CASE SETTINGS

ALPR SETTINGS

ALPR POLICY AND USAGE

Configure Role

DUPLICATE DELETE ROLE

ROLE NAME

TIER

Patrol	Basic
--------	-------

▼ Login Access

Axon Evidence

☐ Allowed ☐ Prohibited

Evidence Sync and Interview Room

☐ Allowed ☐ Prohibited

Axon Capture

☐ Allowed ☐ Prohibited

Axon View XL and Axon Fleet Dashboard

☐ Allowed ☐ Prohibited

Axon App

☐ Allowed ☐ Prohibited

▼ User Access

Edit Account Information

☐ Allowed ☐ Prohibited

View Message Center

☐ Allowed ☐ Prohibited

Download Software

☐ Allowed ☐ Prohibited

Create/Edit Group

☐ Allowed ☐ Prohibited

Group Audit Trail PDF

☐ Allowed ☐ Prohibited

View/Edit User Wi-Fi Networks

☐ Allowed ☐ Prohibited

▼ Admin Access

Configure Agency Security Settings

☐ Allowed ☐ Prohibited

Edit Agency Settings

☐ Allowed ☐ Prohibited

Edit Device Offline & Mic Settings

☐ Allowed ☐ Prohibited

TASER Weapon Logs Administration (manage TASER Weapon logs)

☐ Allowed ☐ Prohibited

Device Administration (register, reassign, and manage non-TASER Weapon devices)

☐ Allowed ☐ Prohibited

Edit Agency Device Settings

☐ Allowed ☐ Prohibited

Edit TASER settings

☐ Allowed ☐ Prohibited

Edit TASER device assignment	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Edit TASER device metadata	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Register TASER devices	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Register TASER, Body 2, and Flex 2 Docks	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
User Administration	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Category Administration	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Return Administration	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
▼ Search & Reporting Access								
User Search	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Partner Contact Search	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
List Unrestricted Evidence	<input type="radio"/>	Any Evidence	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited		
List Restricted Evidence	<input type="radio"/>	Any Evidence	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited		
List Confidential Evidence	<input type="radio"/>	Any Evidence	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited		
Inventory Search			<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited		
List Unrestricted Cases	<input type="radio"/>	Any Case	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited		
List Restricted Cases	<input type="radio"/>	Any Case	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited		
List Confidential Cases	<input type="radio"/>	Any Case	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited		
Generate Reports <small>PRO</small>	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Generate User Audit Trail Report <small>PRO</small>	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
▼ Command Hierarchy								
Manage Command Hierarchy	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
▼ Evidence Creation								
Upload External Files	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
Configure Automatic Upload through Evidence Sync	<input type="radio"/>	Allowed	<input type="radio"/>	Prohibited				
▼ Evidence Management								
View Unrestricted Evidence	<input type="radio"/>	Any Evidence	<input type="radio"/>	Their Groups' & Their Own	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited
View Restricted Evidence <small>PRO</small>	<input type="radio"/>	Any Evidence	<input type="radio"/>	Their Groups' & Their Own	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited
View Confidential Evidence <small>PRO</small>	<input type="radio"/>	Any Evidence	<input type="radio"/>	Their Groups' & Their Own	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited
View TASER Weapon Firing Logs	<input type="radio"/>	Any Evidence	<input type="radio"/>	Their Groups' & Their Own	<input type="radio"/>	Only Their Own	<input type="radio"/>	Prohibited

Edit	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Edit Evidence Group	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Redact PRO	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Auto-Transcribe PRO	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Edit Auto-Transcript PRO	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Verify & Unverify Transcript PRO	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Search across Transcripts PRO			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Start and View People Detection (Coming soon) PRO			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Reassign	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Delete Evidence & Edit Date Recorded	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Download	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Download Infected Files			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Share	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Apply Access Class - Restricted	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Remove Access Class - Restricted	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Apply Access Class - Confidential PRO	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Remove Access Class - Confidential PRO	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Share Externally to Authenticated Users			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Share External Download Links			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Add & Edit Notes	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Audit Trail PDF	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Access Video Recall Files			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Access evidence in their Command			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Access evidence uploaded by Users in their Command			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Manage Content Warning Flag			<input type="radio"/> Allowed	<input type="radio"/> Prohibited
▼ Case Management				
View Unrestricted Cases		<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
View Restricted Cases		<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
View Confidential Cases		<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited

Configure Role

Edit	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Reassign	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Share	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Apply Access Class - Restricted	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Remove Access Class - Restricted	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Apply Access Class - Confidential	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Remove Access Class - Confidential	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Share by Copy with Partner Agencies		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Share External Download Links		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Share by Reference with Partner Agencies	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Audit Trail PDF	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Add & Edit Notes	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Edit Case Retention	<input type="radio"/> Any Case	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Create Case		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
▼ Community Request			
View Portals (Individual, Public, and Incident Report Portals)	<input type="radio"/> Any Portal	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Create Public Portal		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Edit and Close Public Portal	<input type="radio"/> Any Portal	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Create Incident Report Invite		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Edit Incident Report Portals	<input type="radio"/> Any Portal	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Invite Individual		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Triage Submissions	<input type="radio"/> Any Portal	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Audit Trail PDF	<input type="radio"/> Any Portal	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
▼ Axon Respond			
View Map		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
View In-car Locations		<input type="radio"/> All	<input type="radio"/> None
View In-car Livestreams		<input type="radio"/> All	<input type="radio"/> None
View Respond Audit Log		<input type="radio"/> Allowed	<input type="radio"/> Prohibited
Mark Alert As False or Resolved		<input type="radio"/> Allowed	<input type="radio"/> Prohibited

▼ Email Notification Preferences

Account Lockout Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Upcoming Evidence Deletion Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Evidence Timestamp Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Axon Evidence and Performance Service Impact Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Axon Respond for Devices Service Impact Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Axon Respond for Dispatch Service Impact Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Axon Records and Standards Service Impact Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Axon Product Release Notes Notification	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
▼ ALPR			
Read/Hit Record Search	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Hotlist Management	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
ALPR System Administration	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
Read/Hit Record Deletion	<input type="radio"/> Allowed	<input type="radio"/> Prohibited	
▼ Vehicle Assignment			
Fleet 3 Remote User Vehicle Assignment	<input type="radio"/> Any	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited

CANCEL

SAVE

Appendix F

Data Sharing with Other Agencies

Partner Agencies

[Learn More](#)

Optional default sharing recipient not selected

[Set recipient](#)

My Agency Can Receive From

My Agency Can Send To

4 results

ADD AGENCY

Agency Name	City	State	URL	Status ↑	Action
Clay County (MN) Attorney's Office	MOORHEAD	MN	ClayCA.evidence.com	Accepted	
Glyndon Police Dept.	Glyndon	MN	glyndonpdmn.evidence.co...	Accepted	
Moorhead City (MN) Prosecutor's Office	MOORHEAD	MN	moorheadcity.evidence.com	Accepted	
BARNESVILLE POLICE DEPT	Barnesville	MN	barnesvillepdmn.evidence....	Accepted	