RESOLUTION NO. 26-01

CITY OF IRRIGON MUNICIPAL COURT LEDS (LAW ENFORCEMENT DATA SYSTEMS) POLICIES

WHEREAS, The City of Irrigon is charged with providing Public Services for the health and safety; and

WHEREAS, The City of Irrigon Municipal Court has ability and need to use the LEDS system as part of the court's actions; and

WHEREAS, CJIS (Criminal Justice Information System) oversees the LEDS system and requirements, requiring policies to be enacted by the governing body; and

WHEREAS, The following policies are provided for adoption as required by CJIS; and

WHEREAS, The Municipal Court and City Manager may adopt operating procedures in accordance with CJIS and LEDS uses.

NOW, THEREFORE BE IT HEREBY RESOLVED:

The Irrigon Municipal Court and City Manager may adopt operating procedures from time to time in accordance with CJIS and LEDS.

The following policies are adopted for the Irrigon Municipal Court for CJIS and LEDS access, use, and management thereof.

EXHIBIT 1: Storage and Disposal of CJI Information.

EXHIBIT 2: Media Protection Policy

EXHIBIT 3: This resolution shall be effective upon passage.

ADOPTED AND EFFECTIVE BY THE COMMON COUNCIL AND SIGNED ON THIS 21st DAY OF APRIL, 2026.

SIGNED:

Michelle Patton, Mayor

ATTEST:

Aaron Palmquist, City Manager

EXHIBIT 1

Irrigon Municipal Court
Storage and Disposal of CJI Information

PURPOSE

The purpose of this policy is to identify the required protection of Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination or is purged or destroyed in accordance with applicable Oregon State Archives record retention schedules 166-200-0290.

DEFINITIONS

1. Criminal Justice Information (CJI): The abstract term used to refer to all of the FBI Criminal Justice Information Services or other information obtained via the State of Oregon's Law Enforcement Data Systems (LEDS), including any records from Dept of Motor Vehicles provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case or incident history data. In addition, Criminal Justice Information refers to the FBI Criminal Justice Information Services provided data necessary for civil agencies to perform their mission including but not limited to data used to make hiring decisions.

2. Electronic Media: Memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, thumb drives, or digital memory card.

3. Physical Media: Printed documents and imagery that contain Criminal Justice Information.

POLICY

1. The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed, or physically moved from a secure location from the department. This policy applies to any authorized person who accesses, stores, or transports electronic or physical media. Transporting Criminal Justice Information outside the department's assigned physically secure area must be monitored and controlled.

2. Authorized **Irrigon Municipal Court** staff shall protect and control electronic and physical Criminal Justice Information while at rest and in transit. The department will take appropriate safeguards for protecting Criminal Justice Information to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate Criminal Justice Information disclosure or use will be reported to the **Irrigon Municipal Court** Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting, and storing media.

MEDIA STORAGE AND ACCESS

Controls shall be in place to protect electronic and physical media containing Criminal Justice Information while at rest, stored, or actively being accessed. To protect Criminal Justice Information, **Irrigon Municipal Court** staff shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room only accessible to authorized staff.

2. Restrict access to electronic and physical media to authorized staff.

3. Ensure that only authorized staff remove printed form or digital media from the Criminal Justice Information.

4. Physically protect Criminal Justice Information until media end of life. End of life Criminal Justice Information is destroyed or sanitized using approved equipment, techniques, and procedures. (See Destruction Policy)

5. Not use personally owned information system to access, process, store, or transmit Criminal Justice Information.

6. Not utilize publicly accessible computers to access, process, store, or transmit Criminal Justice Information. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

7. Not utilize unsecured, public Wi-Fi for accessing any Criminal Justice Information via City of Irrigon supplied mobile devices, include phones, tablets, or laptops.

8. Store all hardcopy Criminal Justice Information printouts maintained by the department in a secure area accessible to only those employees whose job function requires them to handle such documents.

9. Safeguard all Criminal Justice Information by the department against possible misuse by complying with all Irrigon Municipal Court Acceptable policy

10. Take appropriate action when in possession of Criminal Justice Information while not in a secure area:
    a. Criminal Justice Information must not leave the employee's immediate control. Criminal Justice Information printouts cannot be left unsupervised while physical controls are not in place.

    b. Precautions must be taken to obscure Criminal Justice Information from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock or privacy screens. Criminal Justice Information shall not be left in plain public view. When Criminal Justice Information is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

1) When Criminal Justice Information is at rest (i.e., stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers, and copiers used with Criminal Justice Information. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

2) When encryption is employed, the cryptographic module used shall be certified to meet Federal Standards.

11. Lock or log off computer when not in immediate vicinity of work area to protect Criminal Justice Information. Not all personnel have same Criminal Justice Information access permissions and need to keep Criminal Justice Information protected on a need-to-know basis.

12. Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Criminal Justice Information.

MEDIA TRANSPORT:

Controls shall be in place to protect electronic and physical media containing Criminal Justice Information while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use

1. **Irrigon Municipal Court** staff shall
   a. Protect and control electronic and physical media during transport outside of controlled areas.
   b. Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.
2. **Irrigon Municipal Court** staff will control, protect, and secure electronic and physical media during transport from public disclosure by:
   a. Use of privacy statements in electronic and paper documents.
   b. Limiting the collection, disclosure, sharing and use of Criminal Justice Information.
   c. Following the least privilege and role-based rules for allowing access. Limit access to Criminal Justice Information to only those people or roles that require access.
   d. Securing hand carried confidential electronic and paper documents by:
3. Only viewing or accessing the Criminal Justice Information electronically or document printouts in a physically secure location by authorized personnel.
4. For hard copy printouts or Criminal Justice Information documents:

   • Package hard copy printouts in such a way as to not have any Criminal Justice Information viewable.

   • That are mailed or shipped, **Irrigon Municipal Court** staff must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing Criminal Justice Information material shall be sent by methods that provide for complete shipment tracking and history, and signature confirmation of delivery. This includes the US Postal Service, United Parcel Service, and FedEx.

5. Not taking Criminal Justice Information home or when traveling. When disposing confidential documents, use a cross-cut shredder.

ELECTRONIC MEDIA SANITIZATION AND DISPOSAL:

The department shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). In accordance with DAS policy 107-009-005, the department shall maintain written documentation of the steps taken to sanitize or destroy electronic media. The department shall ensure the sanitization or destruction is witnessed or carried out by authorized staff. Physical media shall be securely disposed of when no longer required, using formal procedures

BREACH NOTIFICATION AND INCIDENT REPORTING:

The department shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including but not limited to audit monitoring, network monitoring, physical access monitoring, and user or administrator reports.

ROLES AND RESPONSIBILITIES:

If information is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. **Irrigon Municipal Court** staff shall notify their supervisor or the **Irrigon Municipal Court** Local Agency Security Officer. A LEDS Security Incident Report form, must be completed and submitted within 24 hours of discovery of the incident. The submitted report shall contain a detailed account of the incident, events leading to the incident, and steps taken or to be taken in response to the incident.

2. Employees will communicate the situation to the **Irrigon Municipal Court** Local Agency Security Officer (LASO) to notify of the loss or disclosure of Criminal Justice Information records.

3. The **Irrigon Municipal Court** Local Agency Security Officer will ensure the CJIS System Agency Information Security Officer and the **Irrigon Municipal Court** Information Security Officer is promptly informed of security incidents.

4. The CJIS System Agency Information Security Officer will:

    a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CJIS System Agency, the affected criminal justice agency, and the FBI CJIS Division Information Security Office major incidents that significantly endanger the security or integrity of Criminal Justice Information.

    b. Collect and disseminate all incident-related information received from the Department of Justice, FBI CJIS Division, and other entities to the appropriate local law enforcement Point of Contacts within their area.

    c. Act as a single point of contact for their jurisdictional area for requesting incident response assistance.

PENALTIES:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and termination.

QUESTIONS:

Any questions related to this policy may be directed to the **Irrigon Municipal Court** Local Agency Security Officer.

IMPLEMENTATION

Each **Irrigon Municipal Court** staff member must take required biennial CJIS training to fully implement this policy.

EXHIBIT 2

Irrigon Municipal Court Media Protection Policy

Policy Title:	Media Protection Policy
Effective Date:	May 2026
Revision Date:	Every 2 years or as needed
Approval(s):	Aaron Palmquist / Thomas Creasing / Amanda Ferguson
LASO:	Thomas Creasing
CSO:	Thomas Creasing/Karma Ezell/Amanda Ferguson
Agency Head:	Aaron Palmquist

Purpose:
The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

This Media Protection Policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy 6.0 dated 12/27/24. The **Irrigon Municipal Court** may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Scope:
The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the **Irrigon Municipal Court** This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized **Irrigon Municipal Court** personnel shall protect and control electronic and physical CJI while at rest and in transit. The **Irrigon Municipal Court** will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the **Irrigon Municipal Court** Local Agency Security Officer (LASO). Procedures shall be defined for secure handling, transporting and storing media.

EXHIBIT 2

Irrigon Municipal Court Media Protection Policy

Media Storage and Access:
Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

To protect CJI, the **Irrigon Municipal Court** personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secure area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Sanitization Destruction Policy)
5. Not using personally owned information system to access, process, store, or transmit CJI unless the **Irrigon Municipal Court** has established and documented the specific terms and conditions for personally owned information system usage. (See Personally Owned Device Policy)
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to; hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the **Irrigon Municipal Court** in a secure area accessible to only those employees whose job function require them to handle such documents.
8. Safeguard all CJI by the **Irrigon Municipal Court** against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.
9. Take appropriate action when in possession of CJI while not in a secure area:
    a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
    b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy

screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.
11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy)

Media Transport:

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The **Irrigon Municipal Court** personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel. .

Irrigon Municipal Court Media Protection Policy

The **Irrigon Municipal Court** personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role-based rules for allowing access. Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
    a. Storing CJI in a locked briefcase or lockbox.
    b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
    c. For hard copy printouts or CJI documents:
        i. Package hard copy printouts in such a way as to not have any CJI information viewable.
        ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)
5. Not taking CJI home or when traveling unless authorized by **Irrigon Municipal Court** LASO. When disposing confidential documents, use a shredder.

Electronic Media Sanitization and Disposal:
The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end-of-life media policy, refer to "Sanitization Destruction Policy".

Breach Notification and Incident Reporting:
The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

EXHIBIT 2

Irrigon Municipal Court Media Protection Policy

Roles and Responsibilities:
If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. **Irrigon Municipal Court** personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
    a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
    b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
    c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

Penalties:
Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Acknowledgement:
I have read the policy and rules above and I will:

- Abide by the **Irrigon Municipal Court's** Media Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Report any **Irrigon Municipal Court** CJI security incident to Supervisor and / or LASO as identified in this policy.

Signature: _____ Date: _____/2026____

Irrigon Municipal Court Media Protection Policy

Questions

Any questions related to this policy may be directed to the **Irrigon Municipal Court's** LASO:

LASO Name: Thomas Creasing	LASO Phone: 541-922-3047	LASO email: thomas.creasing@ci.iurrigon.or.us
State C/ISO Name:	C/ISO Phone:	C/ISO email:

Other Related Policy Reference:

- See Media Sanitization and Destruction Policy
- Media Disposal Policy
- Physical Protection Policy

EXHIBIT 3

Irrigon Municipal Court CJIS Access, Dissemination, and Destruction

	EFFECTIVE: May 2026 **REVISED:**
POLICY HOLDER: Karma Ezell	**POSITION:** Court Clerk

1. Purpose

This policy is meant to ensure that the resource which provides Irrigon Municipal Court staff with criminal justice information (CJI) to perform the city's judicial administrative activities and duties is safeguarded from unlawful and unauthorized use. As CJIS users, employees have access to valuable resources and sensitive data that requires responsible, ethical, and legal behavior.

2. Definitions

Authorized Use: Respecting the rights of all pertinent license and contractual agreements. Users are also subject to federal, state, and local laws.

CJI: Criminal Justice Information

CJIS: CJI System

NLETS: National Law Enforcement Telecommunications Systems

NCIC: National Crime Information Center

Authorized Person: Any person who passed level two, three, or four of the CJIS General or Privileged Roles of the CJIS Awareness tests.

LASO: Local Agency Security Officer (LASO)

3. Scope

This policy covers any authorized person with physical or logical access to CJI.

4. CJIS Access and Dissemination

Policy

Information is available to users from various sources and agencies, including Law Enforcement Database Systems (LEDS) and other state information system files, motor vehicle departments, NCIC, and Oregon State Police Identification Services Section. Each user must observe any restrictions placed on using or disseminating information by its source.

Oregon motor vehicle registration and driving records are the responsibility of the Oregon Department of Transportation, Driver and Motor Vehicle Services Branch (DMV). Oregon government agencies have access to these records via LEDS for authorized criminal justice purposes and licensing, employment, and regulatory purposes expressly permitted by State Law and approved in writing by DMV. Communication, dissemination, or use of this information for other than authorized purposes is prohibited.

National Law Enforcement Telecommunications System (NLETS) Access: NLETS links criminal justice information systems in other states for point-to-point communications between criminal justice agencies and for access to information systems. Access to criminal history records in other states via NLETS is restricted to criminal justice agencies, as defined in Oregon Administrative Rule (OAR) 257-015-0030(5). Access to motor vehicle records in other states and the use of agency-to-agency communication facilities may be limited by NLETS policies or policies in other states.

A. Authorized use does not include inquiries for the collection of taxes and parking violation fees or fines.

B. Authorized uses for Irrigon Municipal Court are defined but not explicitly limited to the following:
    a) Enforcement of state traffic and criminal laws, and regulations;
    b) Review and query driving and registration records for prosecution and sentencing functions.

C. CJI records are temporarily stored on the local server, which only CJIS authorized court employees have access to. Once the records are no longer needed, an authorized court user must delete them from the local drive. All deleted files are backed up and stored on the city's local server, where only the LASO can access and restore them.

D. The Irrigon Municipal Court adheres to and enforces all City of Irrigon city policies and procedures. A copy of these policies can be found online at https://ci.irrigon.or.us/resolutions/. The Irrigon Municipal Court CJI Access, Dissemination, and Destruction Policy refers to the following city policies:
    a) Computer, Network, & Email Acceptable Use
    b) Conduct and Discipline
    c) Telework
    d) Telework Agreement

E. All new hires of the city granted access to the CJIS secured area must pass a CJIS background check within 30 days of hire and pass the CJIS certification test. Employees are expected to recertify every year as required.

F. All new hires of the Irrigon Municipal Court must pass a CJIS background check within 30 days of hire and maintain continuous active CJIS and LEDS certification throughout their career.

G. The Irrigon Municipal Court staff adheres to all rules set forth in the LEDS Manual and CJIS Policy, specifically, but not limited to, the "Use of CJI" section.

H. The Irrigon Municipal Court staff adheres to all existing and future city and administrative regulations as they pertain to CJIS, personal identity information, and other software use policies.

I. Accessing, sharing, or using information for any purpose other than specific job-related criminal justice duties constitutes a violation of this policy.

5. Destruction of CJI

Policy
Maintaining accountability of CJI during destruction includes restricting activities to detect and prevent unnecessary loss or destruction and tampering with CJI.

A. Any authorized person must accompany a third-party document destruction vendor with the shred bin from the authorized CJIS personnel area of city hall to the vendor's destruction area. The authorized person must wait at or near the destruction area until the vendor has emptied the bin so that the authorized person can verify that all CJI has been destroyed properly.

B. Documents containing CJI shall not be stored outside of the CJIS secured area or the locked records cabinet within the records room of city hall.

C. At the end of each work shift, all users must store CJI information in a locked desk drawer or cabinet within the CJIS secured area and consolidate personal shred bins into the larger shred bin located in the authorized CJIS personnel area. This includes all electronic and paper information.

D. All printed CJI material must be destroyed in the shred bin located in the authorized CJIS personnel area.