

RESOLUTION NO. 004-2024

**A RESOLUTION AMENDING APPENDIX 2 H (A POLICY GOVERNING
FINGERPRINT BASED CRIMINAL HISTORY RECORD INFORMATION (CHRI)
CHECKS MADE FOR NON-CRIMINAL JUSTICE PURPOSES) IN THE TOWN OF
CRESTONE MUNICIPAL CODE CHAPTER 2 (ADMINISTRATION)**

WHEREAS, the Board of Trustees of the Town of Crestone, Colorado recognizes the necessity of enacting A Policy Governing Fingerprint-based Criminal History Record Information (CHRI) Checks Made for Non-criminal Justice Purposes; and

WHEREAS Fingerprint-based CHRI checks will only be conducted as authorized by the FBI and CBI, in accordance with all applicable state and federal rules and regulations by "Authorized Personnel" as described in such policy; and

WHEREAS such policy may be amended or supplemented from time to time by resolution of the Board of Trustees.

WHEREAS the Town Board of Trustees agrees to such amendments.

NOW, THEREFORE, be it resolved by the Board of Trustees that the Policy Governing Fingerprint-based Criminal History Record Information (CHRI) Checks Made for Non-criminal Justice Purposes, attached as Exhibit A and incorporated herein by reference is hereby adopted by the Town of Crestone as Appendix 2 H (A Policy Governing Fingerprint-based Criminal History Record Information (CHRI) Checks Made for Non-criminal Justice Purposes) to Chapter 2 (Administration) of the Town of Crestone Municipal Code.

DONE and SIGNED this 8 day of July 2024.


Mayor Benjamin Byer


Interim Town Clerk Arielle Blackwell

Attest:





PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Retention Policy for Criminal History Record Information (CHRI)

Purpose

The purpose of this policy is to establish guidelines for the retention, storage, and security of Criminal History Record Information (CHRI) to ensure the confidentiality and integrity of these records while complying with applicable laws and regulations.

Scope

This policy applies to all employees, contractors, and third-party service providers who handle CHRI on behalf of the agency.

Policy Statement

The agency is committed to safeguarding CHRI through appropriate administrative, technical, and physical safeguards. CHRI shall be stored only for as long as necessary to maintain the integrity and utility of case files and/or criminal record files. The retention period for CHRI shall not exceed two years.

Retention Period

1. Standard Retention Period:

- CHRI shall be stored for a minimum of one year and a maximum of two years from the date of receipt or creation.

2. Extended Retention Period:

- CHRI may be retained beyond the standard period only if it is a key element for the integrity and/or utility of case files and/or criminal record files. Such determinations must be documented and approved by authorized personnel.

Safeguards

1. Administrative Safeguards:

- Access to CHRI shall be restricted to authorized personnel only.
- Regular training shall be provided to all employees handling CHRI on data protection and confidentiality.
- An access log shall be maintained to track who accessed CHRI and when.

2. Technical Safeguards:

- CHRI shall be stored in secure, encrypted databases.
- Strong authentication mechanisms shall be employed to prevent unauthorized access.
- Regular audits shall be conducted to ensure compliance with security protocols.

3. Physical Safeguards:

- CHRI shall be stored in secure, locked facilities.
- Access to physical storage areas shall be restricted to authorized personnel.

Compliance with CJIS Security Policy

This policy adheres to the requirements set forth in the Criminal Justice Information Services (CJIS) Security Policy, specifically:

- Section 5.9 Physical Protection: Ensuring the physical protection of CHRI through restricted access and secure storage facilities.
- Section 4.2.4 Storage: Ensuring that CHRI is stored in a secure manner, utilizing encryption and other technical safeguards.

Disposal of CHRI

At the end of the retention period, CHRI shall be securely disposed of in a manner that ensures the information cannot be reconstructed or retrieved. Disposal methods may include:

- Shredding of physical documents.
- Secure deletion of electronic records.

Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Any breaches of CHRI security shall be reported immediately to the designated compliance officer.

Review and Revision

This policy shall be reviewed annually and updated as necessary to reflect changes in legal requirements and organizational practices.

This policy is effective as of 1 June 2024.



Arielle Blackwell, Interim Town Clerk

1 June 2024





PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Disciplinary Policy for Misuse of Sensitive Information Including Criminal History Record Information (CHRI)

1. Purpose

The purpose of this policy is to establish guidelines for the disciplinary actions that will be taken in the event of misuse of sensitive information, including Criminal History Record Information (CHRI). This policy ensures compliance with state statutes and Federal code, as well as the CJIS Security Policy.

2. Definition of Misuse

Using CHRI for any purpose other than what is explicitly allowed by state statute or Federal code is considered misuse. Misuse includes, but is not limited to:

- Accessing CHRI for personal reasons or curiosity
- Sharing CHRI with unauthorized individuals
- Using CHRI for any unauthorized purpose

3. Procedures for Addressing Misuse

In the event that intentional misuse of CHRI is discovered, the following steps will be taken:

3.1 Initial Investigation

- An initial investigation will be conducted to determine the validity of the misuse claim.
- The individual accused of misuse will be temporarily suspended from access to CHRI pending the outcome of the investigation.

3.2 Reporting

- Misuse of CHRI shall be reported to the appropriate state authorities as required by law.

3.3 Disciplinary Actions

Depending on the findings of the investigation, the following disciplinary actions may be taken:

3.3.1 Loss of Access

- The individual found to have misused CHRI will permanently lose access to CHRI.

3.3.2 Employment Actions

- Misuse of CHRI can result in disciplinary actions up to and including termination of employment.

3.3.3 Criminal Prosecution

- Misuse of CHRI may result in criminal prosecution, in accordance with state and Federal laws.

4. Compliance

This policy complies with the CJIS Security Policy, Section 5.12.4 Personnel Sanctions. All employees are required to adhere to this policy, and failure to do so will result in disciplinary action as outlined above.

5. Training and Awareness

All employees with access to CHRI will receive training on the proper use and handling of this information, as well as the consequences of misuse.

6. Policy Review

This policy will be reviewed annually to ensure it remains current with state statutes, Federal codes, and CJIS Security Policy.

7. Effective Date

This policy is effective as of June 1, 2024.

By implementing and adhering to this disciplinary policy, our agency aims to ensure the proper use and protection of sensitive information, maintaining the highest standards of security and integrity.





PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Destruction Policy for Physical/Printed Criminal History Record Information (CHRI)

Purpose

The purpose of this policy is to establish formal procedures for the secure disposal and destruction of physical/printed Criminal History Record Information (CHRI) to minimize the risk of sensitive information compromise by unauthorized individuals. This policy is in compliance with CJIS Security Policy, Section 5.8 MP-6 Media Sanitization.

Scope

This policy applies to all physical/printed CHRI maintained by our office.

Policy

1. Destruction Schedule

- Physical/printed CHRI shall be securely destroyed when it is no longer required for operational purposes or upon the completion of its retention period as specified by relevant laws, regulations, and office policies.

2. Methods of Destruction

- Physical media containing CHRI shall be destroyed by shredding or incineration. The chosen method must ensure that the information is rendered unreadable and irrecoverable.

3. Shredding Procedure

- Shredding of CHRI documents shall be performed using cross-cut shredders that produce particles no larger than 5mm x 30mm.
- Shredded materials shall be disposed of in a manner that ensures they cannot be reconstructed or read.

4. Incineration Procedure

- If incineration is chosen as the method of destruction, it shall be conducted in a secure and controlled environment.
- The incineration process must ensure complete combustion of the documents.

5. Authorization and Witnessing

- Disposal or destruction of CHRI shall be carried out or witnessed by authorized personnel.
- Authorized personnel must have undergone proper training on the handling and destruction of CHRI.

6. Record Keeping

- A destruction log shall be maintained, documenting the date of destruction, the method of destruction, a description of the records destroyed, and the names of the personnel involved.
- The destruction log shall be retained for a minimum of five years.

7. Digital Copies

- Any digital copies of CHRI shall be erased permanently using secure erasure methods compliant with industry standards to ensure that data cannot be recovered.

Responsibilities

- Authorized Personnel: Ensure that physical/printed CHRI is destroyed securely and in accordance with this policy.
- Clerk: Oversee the implementation of this policy and maintain the destruction log.

Compliance

Non-compliance with this policy may result in disciplinary action and potential legal consequences. All personnel handling CHRI must adhere to this policy to ensure the security and confidentiality of sensitive information.

Review and Updates

This policy shall be reviewed annually and updated as necessary to reflect changes in laws, regulations, and office procedures.

Approved by: Interim Town Clerk Arielle Blackwell

1 June 2024





PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Incident Handling Procedures for CHRI Repository

1. Preparation

- Training: Regularly train staff on recognizing and responding to security incidents.
- Documentation: Maintain up-to-date documentation of incident response plans and procedures.
- Tools: Ensure the availability and proper functioning of necessary tools and software for incident detection and analysis.
- Communication Plan: Establish a clear communication plan outlining the roles and responsibilities of the response team and reporting protocols.

2. Detection

- Monitoring: Implement continuous monitoring of systems and networks to identify potential security incidents.
- Alerts: Set up automated alerts for suspicious activities such as unauthorized access attempts, unusual data transfers, or system anomalies.
- User Reports: Encourage users to report any unusual or suspicious activities immediately.

3. Analysis

- Initial Assessment: Quickly assess the nature and scope of the incident to determine its impact on the CHRI repository.
- Evidence Gathering: Collect and preserve all relevant evidence, including logs, system snapshots, and user reports.

- Incident Classification: Classify the incident based on its severity, type, and potential impact on CHRI data.

4. Containment

- Immediate Action: Take immediate steps to contain the incident and prevent further damage, such as isolating affected systems, disabling compromised accounts, or blocking malicious IP addresses.
- Short-term Containment: Implement short-term measures to mitigate the impact while planning for long-term solutions.
- Communication: Inform relevant stakeholders, including agency officials and affected users, about the containment actions taken.

5. Recovery

- System Restoration: Restore affected systems to normal operations, ensuring that any vulnerabilities are addressed to prevent recurrence.
- Data Integrity: Verify the integrity of CHRI data and ensure no unauthorized modifications have occurred.
- Monitoring: Continue monitoring systems closely to detect any signs of residual malicious activity.

6. User Response Activities

- Notification: Notify users whose data may have been compromised, providing them with guidance on protective measures.
- Support: Offer support to affected users, including resources for identity protection and credit monitoring if necessary.
- Education: Educate users on how to recognize and respond to future security threats.

7. Documentation

- Incident Report: Document all details of the incident, including the timeline of events, actions taken, and evidence collected.
- Analysis: Conduct a thorough analysis of the incident to identify root causes and contributing factors.
- Lessons Learned: Document lessons learned and update incident response plans and procedures accordingly.

8. Reporting

- Internal Reporting: Report the incident to appropriate agency officials, including details on the nature, impact, and response actions taken.
- External Reporting: If required, report the incident to external authorities, such as law enforcement or regulatory bodies, in accordance with CJIS Security Policy.
- Follow-up: Follow up on reported incidents to ensure that necessary actions have been taken and to address any additional concerns.



PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Acceptable Use Policy for Criminal History Record Information (CHRI)

Purpose

This Acceptable Use Policy (AUP) is established to ensure that Criminal History Record Information (CHRI) is used solely for the official purpose for which it was requested, specifically to conduct background checks through the national criminal history records of the FBI. This policy is in accordance with Public Law 92-544 and Title 28, C.F.R., 20.33 and 50.12(b). The policy outlines the acceptable use, security, and confidentiality measures to be adhered to by all personnel handling CHRI.

Scope

This policy applies to all employees, contractors, volunteers, and any other individuals who have access to CHRI in the course of their duties.

Policy Statements

1. Authorized Use

- CHRI shall be accessed and used only for the official purpose of conducting background checks as authorized by relevant laws and regulations.
- Unauthorized access, use, or dissemination of CHRI is strictly prohibited.

2. Access Control

- Access to CHRI is restricted to authorized personnel who have undergone appropriate background checks and training.

- Users must utilize unique user IDs and passwords to access CHRI systems. Sharing of login credentials is prohibited.

3. Confidentiality

- CHRI must be treated as confidential and must not be disclosed to unauthorized individuals or entities.

- Information obtained from CHRI must not be used for personal or non-official purposes.

4. Data Security

- CHRI must be stored and transmitted securely to prevent unauthorized access, modification, or destruction.

- Electronic CHRI must be protected using encryption and other relevant security measures. Physical CHRI must be stored in locked, secure locations.

5. Training

- All personnel authorized to access CHRI must complete mandatory training on the proper use, handling, and security of CHRI.

- Regular refresher training must be conducted to ensure ongoing compliance with this policy.

6. Monitoring and Auditing

- Access to and use of CHRI shall be monitored and audited regularly to ensure compliance with this policy.

- Any suspicious activity or violations of this policy must be reported immediately to the designated security officer.

7. Incident Reporting

- Any incidents involving the unauthorized access, use, or disclosure of CHRI must be reported promptly to the appropriate authorities.

- Affected individuals must be notified as required by law or policy.

8. Disciplinary Actions

- Violations of this policy may result in disciplinary actions, up to and including termination of employment or contractual agreements and may also result in legal action.

9. Review and Updates

- This policy shall be reviewed annually and updated as necessary to ensure it remains current with applicable laws, regulations, and best practices.

Responsibilities

- Local Agency Security Officer (LASO): Responsible for overseeing the implementation of this policy, conducting audits, and investigating any reported incidents.
- Authorized Users: Responsible for complying with this policy, completing required training, and reporting any security incidents or policy violations.

Acknowledgment

All personnel authorized to access CHRI must sign an acknowledgment form indicating they have read, understood, and agree to comply with this Acceptable Use Policy.

By adhering to this policy, we ensure that CHRI is used responsibly, securely, and in accordance with legal and ethical standards. This safeguards the integrity of the background check process and protects the privacy of individuals whose information is being accessed.



PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Media Protection Policy

Purpose

The purpose of this Media Protection Policy is to ensure that both physical and electronic media are handled, transported, and stored securely. This policy aims to protect sensitive information from unauthorized access, disclosure, alteration, or destruction.

Scope

This policy applies to all employees, contractors, and authorized personnel who handle, transport, or store physical or electronic media.

Policy

This policy is established in accordance with the CJIS Security Policy, Section 5.8 MP-1 Media Protection Policy and Procedures.

1. Access Control

- Access to all forms of media shall be restricted to authorized individuals only.
- Authorization levels shall be defined based on the sensitivity of the media and the role of the individual.
- Access logs shall be maintained for tracking purposes.

2. Handling Procedures

- Media shall be handled with care to prevent unauthorized access or damage.

- Sensitive media shall be labeled appropriately.
- Electronic media must be encrypted where applicable.
- Employees must avoid leaving sensitive media unattended.

3. Transport Procedures

- Media shall be transported using secure methods to prevent unauthorized access or loss.
- When transporting physical media:
 - Use sealed, tamper-evident packaging.
 - Transport by trusted personnel or secure courier services.
- When transporting electronic media:
 - Use encrypted devices or secure file transfer methods.
 - Ensure that the recipient is authorized to receive the media.

4. Storage Procedures

- Physical media:
 - Store in locked, secure areas with restricted access.
 - Use fireproof and waterproof containers for highly sensitive media.
- Electronic media:
 - Store on secure servers with access controls and encryption.
 - Regularly back up data and store backups in a separate, secure location.

5. Disposal Procedures

- Media containing sensitive information must be disposed of securely.
- Physical media:
 - Use shredding, incineration, or other methods to ensure complete destruction.

- Electronic media:
 - Use data wiping tools or physical destruction to ensure data cannot be recovered.

6. Training and Awareness

- All personnel handling media shall receive training on this policy and related procedures.
- Regular refresher courses and updates on new threats and security measures shall be conducted.

7. Incident Management

- Any incidents involving the unauthorized access, loss, or damage of media must be reported immediately.
- An incident response team shall investigate and take appropriate actions to mitigate risks and prevent future occurrences.

Responsibilities

- Local Agency Security Officer (LASO): Ensures policy compliance and conducts regular audits.
- Department Managers: Implement and enforce this policy within their departments.
- Employees and Contractors: Adhere to the policy and report any incidents or breaches.

Review and Revision

This policy shall be reviewed annually or when significant changes occur in the organization or regulatory environment.

Approval

This Media Protection Policy has been approved by the organization's management and is effective as of 1 June 2024.

Effective Date: 1 June 2024

Approved by: Interim Town Clerk Arielle Blackwell

Revision History:

- 1 June 2024 - Initial policy creation.
- [TBD] - First revision.



PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Physical Protection Policy

Purpose

This policy establishes the procedures for ensuring that Criminal History Record Information (CHRI) and associated hardware, software, and media are accessible only by authorized personnel within the Town of Crestone. The goal is to protect sensitive information and equipment from unauthorized access, theft, or damage, in compliance with the CJIS Security Policy, Section 5.9 - Physical Protection.

Scope

This policy applies to all employees, contractors, and third-party personnel who have access to CHRI and related hardware, software, and media within Town of Crestone.

Policy

1. Secure Areas and Controlled Access

- Clerk's Room: CHRI and associated hardware (including Live Scan machines), software, and media must be stored and processed in the Clerk's room, which is a designated secure area. The Clerk's room is locked and only accessible to authorized personnel.
- Locked Drawer: Within the Clerk's room, CHRI must be stored in a locked drawer. Only authorized personnel should have access to the keys for this drawer.

2. Access Authorization

- Authorization Process: Access to the Clerk's room and the locked drawer where CHRI is stored is granted only to individuals who have been vetted and authorized by the Town of

Crestone. The authorization process includes background checks, CHRI-specific training, and approval from management.

- Access Lists: Maintain an up-to-date list of personnel authorized to access the Clerk's room and the locked drawer. This list should be reviewed and updated regularly to reflect any changes in personnel or access needs.

3. Physical Security Measures

- Locking Mechanisms: Ensure that the door to the Clerk's room and the drawer storing CHRI are equipped with sturdy locks. Only authorized personnel should have keys or access codes.
- Surveillance: Implement surveillance measures, such as security cameras, to monitor the Clerk's room. Surveillance footage should be reviewed regularly to detect any unauthorized access attempts.
- Alarm Systems: Install alarm systems to alert security personnel of any unauthorized entry or suspicious activity in the Clerk's room.

4. Access Control Procedures

- Identification: Require all personnel entering the Clerk's room to display proper identification at all times. Visitors should be escorted by authorized personnel and logged in a visitor access log.
- Access Logs: Maintain access logs to record the entry and exit of personnel in the Clerk's room. Logs should include the name of the individual, time of access, and purpose of visit. These logs should be reviewed periodically to ensure compliance with access control policies.

5. Handling and Storage of CHRI

- Secure Storage: CHRI must be stored in a locked drawer within the locked Clerk's room when not in use. Ensure that only authorized personnel have access to keys or combinations.
- Processing Areas: CHRI should only be processed in the Clerk's room. Avoid processing CHRI in public or unsecured locations.
- Media Protection: Any media containing CHRI, such as USB drives, CDs, or printed documents, must be securely stored and labeled. Media should be encrypted where possible and access should be limited to authorized personnel.

6. Incident Response

- Reporting: Immediately report any suspected or confirmed unauthorized access, theft, or loss of CHRI, hardware, software, or media to the security team and management.
- Investigation: Conduct a thorough investigation of all incidents involving unauthorized access or loss of CHRI. Take appropriate corrective actions to prevent future occurrences.
- Documentation: Document all incidents and responses in an incident log. This log should be reviewed regularly to identify trends and areas for improvement.

7. Training and Awareness

- Training Programs: Provide regular training to all personnel on physical protection policies and procedures related to CHRI. Training should include information on identifying and reporting security incidents, proper handling and storage of CHRI, and access control measures.
- Awareness Campaigns: Conduct awareness campaigns to reinforce the importance of physical protection and security measures. Use posters, newsletters, and other communication channels to remind personnel of their responsibilities.

Compliance and Enforcement

Failure to comply with this Physical Protection Policy may result in disciplinary action, up to and including termination of employment. The Town of Crestone reserves the right to audit compliance with this policy and take necessary corrective actions.

Review and Revision

This policy will be reviewed annually and updated as necessary to ensure continued effectiveness and alignment with organizational and regulatory requirements.

Approval

This policy is approved by:



Arielle Blackwell

Interim Town Clerk

1 June 2024





PO Box 64, Crestone, CO 81131 • (719) 256-4313 • crestonetownoffice@gmail.com

Privacy Statement for Job Applicants

By signing this document, I acknowledge that I have received and reviewed this privacy statement. I understand that as part of the application process for employment, my ~~fingerprints~~ will be taken and used to check the national criminal history records of the FBI.

In accordance with Title 28 CFR 50.12 (b), I understand that the information obtained from the ~~fingerprinting and~~ background check will be used solely to make a decision regarding my employment with the Town of Crestone. This information will be retained for a period of one to two (1-2) years and will not be shared with the public.

I acknowledge that I have read and understand the above statement and agree to the terms and conditions outlined herein.

Applicant's Signature: _____

Printed Name: _____

Date: _____