Policy Number:
46
Effective Date: 10/11/22
Revised: 5/13/25

Subject: Access & Use of Fingerprint-Based Criminal History Record Information & Incident/Security Response

PURPOSE:

Camden County Developmental Disability Resources (CCDDR) recognizes the need to comply with Federal, State, and local laws/regulations regarding employee and volunteer criminal background information. The purpose of this policy is to comply with all laws and regulations.

POLICY:

Criminal History Information (CHRI) and Criminal Justice Information (CJI) must be accessed and used correctly and destroyed in accordance with record retention rules. This applies to all electronic or paper records containing FBI CJI or CHRI being stored, accessed, or physically moved from a secure location of CCDDR. This also applies to any authorized individual accessing, storing, and/or transporting electronic or paper records. The Local Agency Security Officer (LASO) will keep a list of users having access to the CJIS system as well as a file of those having access to information received from CJIS Services.

In accordance with the National Child Protection Act of 1993, as amended; RSMo 630.170; and 9 CSR 10-5.190, CCDDR conducts a state and national fingerprint-based criminal background check on all new employees, contractors working directly with clients, and volunteers.

A basic security and privacy training is required for all employees authorized to access Criminal Justice Information (CJI) before accessing the system, information, or performing assigned duties and annually thereafter. The CCDDR employee/employees complete the security awareness training online, and proof of the training is kept for a minimum of three years in the employee's personnel file.

Before being fingerprinted, the employee or volunteer must be given a copy of the "Noncriminal Justice Applicant's Privacy Rights" and the FBI's "Privacy Act Statement", which employees or volunteers may keep for their records. The employee or volunteer are also given a copy of the "Missouri Applicant Fingerprint Privacy Notice" and the "MoVechs Waiver Agreement and Statement", which must be signed, dated, and retained in the employee's personnel file. CCDDR will ensure the CHRI received for each employee is protected from time of receipt to time of destruction.

CCDDR strives to ensure that all employee personnel records are secure and locked in a file cabinet and only authorized individuals are allowed access to the personnel files. Improper

access, use and dissemination of data received is serious and could result in termination of employment. Misuse of this information is a Class A misdemeanor.

When a security incident is reported, the information is ONLY used to perform the required job duty. Never share information with anyone that is not authorized to have access to the information. CCDDR WILL NOT DISSEMINATE criminal history or criminal justice information!

A security violation is the act of violating, knowingly or not, a security policy regarding CHRI. Security violations include but are not limited to: CHRI systems/data misuse; virus/malware/ransomware attacks; network intrusion; data loss/data breach; unauthorized access to CHRI systems, denial of service; unauthorized changes; and theft/loss of devices containing CHRI.

This Incident/Security Response Policy shows steps to be taken in the event personnel files are destroyed or an unauthorized individual gains access to sensitive personally identifiable information received from the MSHP regarding background checks.

In the event someone attempts to gain unauthorized access to the system or data received from the system, the following steps are to be taken as soon as the incident is reported:

1. The individual discovering the Incident will immediately call the LASO or those having authorization or access to the information and report the following information:

    - Date and time the incident was discovered
    - Location of the incident
    - Nature of the incident
    - Who reported the incident
    - How the incident was detected

2. The incident will be reported to the Executive Director by the LASO or those having authorization or access to the information

3. The LASO or those having authorization or access to the information will fill out the Missouri State Highway Patrol Security Incident Report Form SHP71 and call the MSHP at 573-522-3820 after form is filled out and fax to 573-526-6290, Missouri State Highway Patrol Criminal Justice Information Services (CJIS) Security Unit. or e-mail to cjissecurity@mshp.dps.mo.gov within 24 hours of the incident. For questions call 573-526-6153 ext. 2658.

The Incident/Security Response Policy was developed to meet the following objectives:

- Prevent unauthorized viewing of sensitive information
- Provide an organized approach to managing initial response following an incident
- Provide prompt and appropriate response to incidents

- Notify appropriate management and/or operational staff of the incident

The “dos” and “don’ts” of sensitive, personally identifiable information are:

1. Do not store information on flash drives, hard disks, CDs, DVDs, or any electronic media.
2. Store all information in locked cabinets, and access is granted to authorized personnel only.
3. Do not transport information unless the information is in locked container.
4. When destroying information, physically destroy, shred, or burn.
5. Do not use laptops, tablets, or handheld devices.
6. Do not share user identifications or passwords or write them down.
7. Do not send CJIS information in an e-mail. (Personal devices are not allowed to access information – devices need to be secure and password protected.)

Information needs to be protected from creation to destruction, and there must be awareness of the information flow. Information must be given to an authorized employee, information must be protected, and computer security incidents must be reported immediately. Extreme caution must be observed and recognized when someone is asking for information.

In the event of an incident, the Missouri State Highway Patrol (MSHP) Security Incident Report is to be filled out in full and submitted to the MSHP as well as calling them to report the incident within 24 hours of the incident.

Only authorized employees have access or can view CHRI and are NOT to share or disclose the information to unauthorized employees. IF CHRI is in a printed format, authorized employees will ensure the information is in locked file cabinets and not accessible by any unauthorized employees. If CHRI is stored electronically or on a local hard drive, it must be password protected or encrypted. An in-house cross shredder must be used to destroy information of CHRI. If an electronic copy CHRI is stored on HDDS or flash drives, the electronic media must be degaussed a minimum of three times.

CCDDR will make certain all MACHS portal access is up to date and anyone not needing access is removed within 24 hours by the LASO or MACHS administrator. The LASO will contact the MSHP, CJIS Division for administrator’s rights to the MACHS portal. Documentation must be retained for audit purposes to prove MACHS portal access was removed within 24 hours of termination.

CCDDR will also ensure that Missouri and national Rap Back subscriptions are discontinued within 5 business days of an employee’s termination. Subscriptions for contractors should be discontinued as soon as the agency is notified that the contractor’s services are no longer needed. Documentation must be retained for audit purposes to prove termination of the subscriptions occurred within 5 business days. Rap Back subscriptions and validations will be completed by the LASO or Human Resources designee.