



NONCRIMINAL JUSTICE AGENCY USE OF CRIMINAL JUSTICE INFORMATION

**PRESENTED BY:
MICHIGAN STATE POLICE
CRIMINAL JUSTICE INFORMATION CENTER
SECURITY & ACCESS SECTION**

**“A PROUD tradition of SERVICE through EXCELLENCE, INTEGRITY, and
COURTESY”**



Security & Access Team



Staff Members:

Larry Jones, Manager

Narcisa Morris, Analyst

Sandy Billingsley, Analyst

Joe Diaz, Analyst

Security & Access Section (SAS) E-Mail:

MSP-CJIC-ATS@michigan.gov



Criminal Justice Information



What is Criminal Justice Information (CJI)?

- CJI is the term used to describe all of the FBI Criminal Justice Information Services (CJIS) provided data necessary for civil agencies to perform their employment or volunteer placement determinations.

What is Criminal History Record Information (CHRI)?

- A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual, as well as the disposition of any charges.



Criminal Justice Information Exchange History

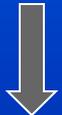


FBI Criminal Justice Information Services



Serves as the nation's administrator for the appropriate security and management controls. As such, the FBI designates one criminal justice agency (on the CJIS network) as the CJIS Systems Agency (CSA) and is considered a point of contact in each state.

Michigan State Police



The CSA is duly authorized to oversee the security and management of all CJI exchanges within the State of Michigan. **Responsible for setting, maintaining, enforcing, and reporting compliance to the FBI CJIS Division for such exchanges.

Noncriminal Justice Agency

For the purpose of licensing and employment, certain authorized agencies request and receive fingerprint-based CHRI, making the NCJAs the next responsible records management entity.

**Title 42 U.S.C., Chapter 140, Subchapter II, 14616; 28 CFR Part 901 § 4, requires MSP SAS to complete NCJA compliance audits.



NCJA Audit Information Sheet



NONCRIMINAL JUSTICE AGENCY COMPLIANCE AUDIT REVIEW INFORMATION SHEET

Federal statute and section number references from the FBI CJIS Security Policy are available after each policy section for details on the particular subject matter.

The following areas will be covered in the compliance audit:

Supporting Documentation

- Fingerprint Authorization
- Position Documentation
- Consent
- Appeal

User Agreements (5.1.1.6)

Local Agency Security Officer LASO (3.2.9)

Personnel Security (5.12)

Media Protection (5.8)

Physical Protection (5.9)

Secondary Dissemination (5.1.3)

Security Awareness Training (5.2.1.1)

Incident Response (5.3)

Compliance Audit Contact Information:

Security & Access Section E-mail: MSP-CJIC-ATS@michigan.gov

Narcisa Morris, Auditor	MorrisN@michigan.gov	(517) 420-2329
Sandra Billingsley, Auditor	BillingsleyS@michigan.gov	(517) 242-1944
Joe Diaz, Auditor	diazj6@michigan.gov	(517) 507-9705

CHR Questions

Out of state CHRI questions must be directed to the state of record. If you have a Michigan CHRI question, please refer to www.michigan.gov/ichat Tutorial-"How to read a criminal history (CH)." Questions regarding Livescan, NCJA User Agreements, or State portion of the CHRI responses may be directed to the Criminal History Section (CHS) applicant help desk at (517) 241-0606 or by e-mail, msp-crd-applhelp@michigan.gov.

ICHAT Questions

[Questions or comments \(517\) 241-0713 or by e-mail msp-crd-ichathelp@michigan.gov.](mailto:msp-crd-ichathelp@michigan.gov)

The Following Official Forms and Documents Can Be Located At Our Web Page

> www.michigan.gov/cjicats

Livescan Fingerprint Request RI-030

Noncriminal Justice Agency (NCJA) User Agreement for Release of Criminal History Record Information (CHRI) RI-087

Noncriminal Justice Agency (NCJA) Local Agency Security Officer Appointment CJIS-015

Information Security Officer (ISO) Computer Security Incident Response Capability Reporting CJIS-016

NCJA CHRI Policy template (doc)

[Agency] Appeal Process template

FBI Criminal Justice Information Services (CJIS) Security Policy website link

MSP Security Awareness Training Template (PowerPoint)

Secondary Dissemination Log

Unknown CHRI Response Log

Q&A (doc)



Fingerprinting Authorization

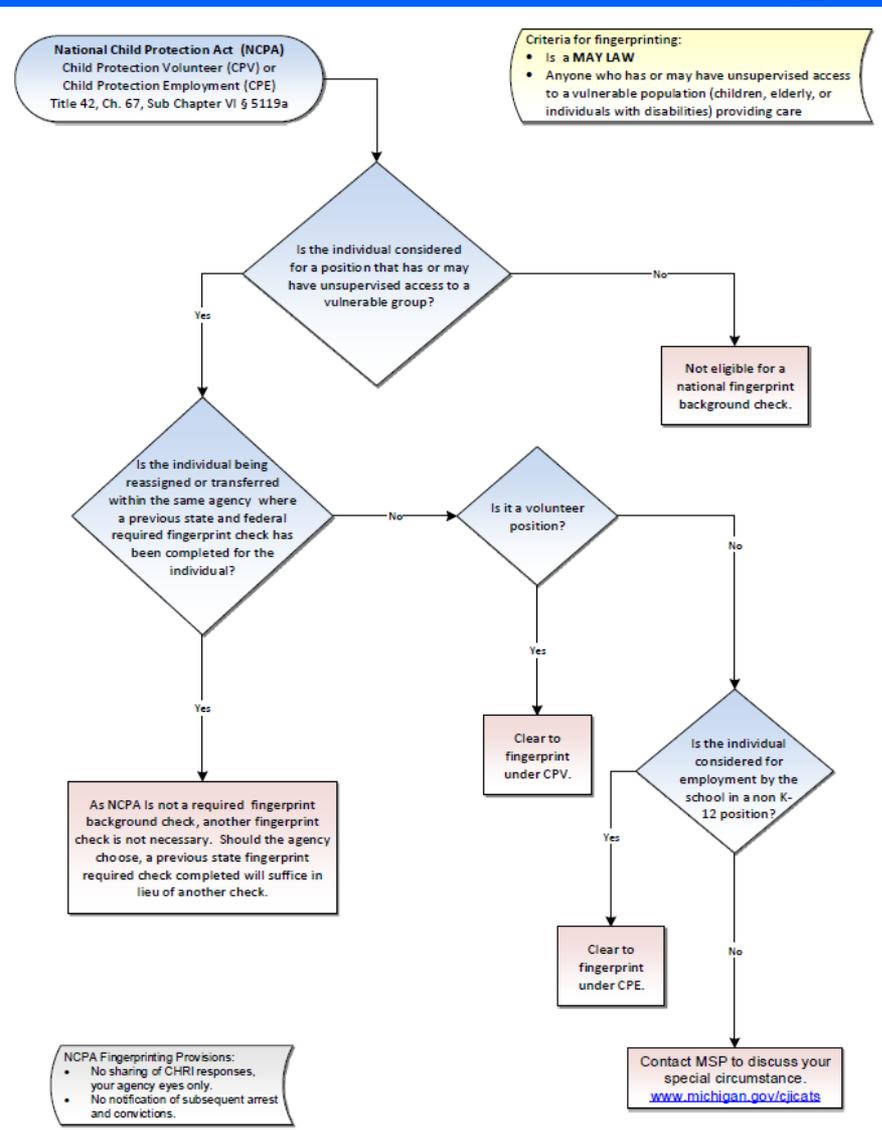
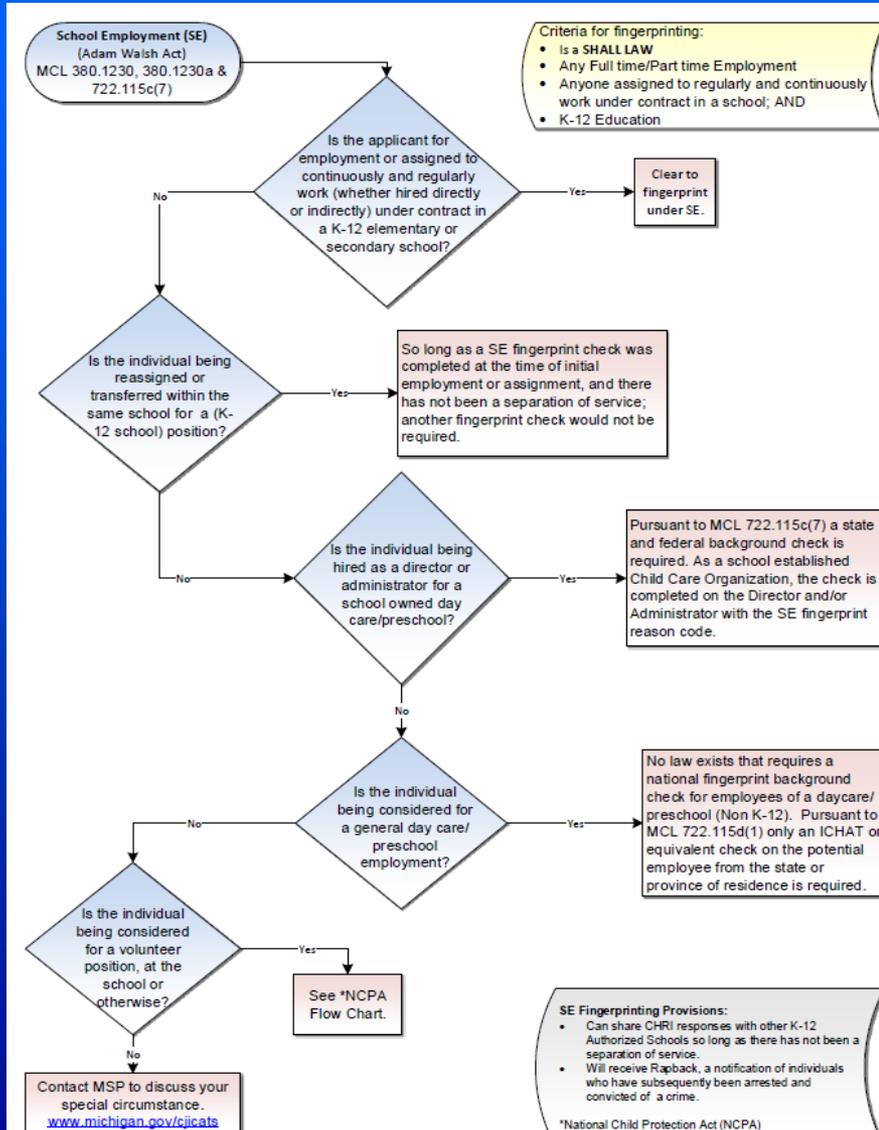


The following are federal and state laws authorizing fingerprint-based CHRI background checks for employment, licensing, or volunteer determinations:

- School Employment (SE)/Adam Walsh Act (AWA); MCL 380.1230a, The Revised School Code (**SHALL**)
- National Child Protection Act Employment (CPE) & Child Protection Volunteer (CPV); 42 USC 5119 § 320928 & National Child Protection Act, including volunteers (**MAY**)



Flow Charts





NCJA Audits



NCJA will receive an email notification to the contact and email provided when the agency established their fingerprinting account. The notification will:

- Provide you the date and time of your agency audit.
- Provide instruction for completing our online NCJA PreAudit Questionnaire.
- Provide instruction on your participation for the compliance audit review.
- Provide your agency with details on what to expect.

A screenshot of the Michigan State Police CJIS Audit interface. The page has a white background with a grey header bar. The header bar contains the text "Michigan State Police" on the right and a logo on the left consisting of a checkmark icon and the text "CJIS Audit". Below the header bar is a large white area. On the left side of this area is the Michigan State Police logo. On the right side are two rounded rectangular buttons: "Agency Login" and "FullAdmin Login". Below the "FullAdmin Login" button is a small mouse cursor icon. At the bottom of the white area is the text "Launch Pad Home". At the very bottom of the page is a grey footer bar containing the text "powered by Peak Performance Solutions" and a logo of a person with arms raised. Below the footer bar is the text "Copyright © 2016 Peak Performance Solutions".



Supporting Documentation

(1 of 4)



SAS Audit Criteria:

- Random fingerprint sample:
 - An agency “fingerprint sample” is an Excel spreadsheet report, which consists of a list of individual names requested to complete a fingerprint background check for employment or volunteerism under your Agency ID.



Supporting Documentation

(2 of 4)



SAS Audit Criteria Continued:

- Position documentation for the fingerprint reason code used by the agency.
 - Documentation which indicates the fingerprint-based CHRI background checks obtained are for a specific purpose authorized by state or federal law. Position documentation:
 - Is individualized
 - Provides the individual's name
 - Provides the position offered by the agency

This documentation can be easily identified as a document used during your agency's hiring process. (i.e. employment contracts, new hire checklist, letter of hire, determination for assignment etc.).



Red Light–Green Light Example



[AGENCY NAME]

DETERMINATION FOR ASSIGNMENT

(L Name, F Name Middle Initial)

(Contact Number)

(Position Assigned)

Based on the information we have obtained on the above named individual, we are making the following determination:

_____ Yes, the individual is cleared to work in a Michigan school.

_____ Yes, the individual is cleared to work in a Michigan school. However, based on additional district/school policy and guidelines of [AGENCY NAME], we will not be accepting the individual for assignment at our district/school.

_____ No, the individual is not cleared to work in a Michigan school.

I state I am authorized to make this determination for our district and have based my determination on current district/school policies and guidelines and current Michigan law. I understand that I am responsible to notify [CONTRACTING ENTITY] in writing if there is a change in this determination.

Printed Name & Title

Signature

Approval Date



Supporting Documentation

(3 of 4)



SAS Audit Criteria Continued:

Livescan fingerprinting RI-030 is a multi-purpose required form.

- Fingerprinting Consent:
 - Is the properly signed and dated Livescan RI-030 request form. This is an individual's consent to be fingerprinted and is given *prior* to fingerprinting.
 - www.michigan.gov/cjicats (Forms)



LIVESCAN FINGERPRINT REQUEST FORM RI-030



RI-030 (09/2015)
MICHIGAN STATE POLICE

LIVESCAN FINGERPRINT BACKGROUND CHECK REQUEST

AUTHORITY: MCL 28.162, MCL 28.214, MCL 28.248, & MCL 28.273; **COMPLIANCE:** Voluntary. However failure to complete this form will result in denial of request.

Purpose: To conduct a fingerprint based background check for employment, to volunteer, or for licensing purposes as authorized by law.

I. Authorizing Information: Please ensure the correct fingerprinting reason code and agency ID are used. The Michigan State Police (MSP) will charge for second requests due to incorrect codes.

1. Fingerprint Code	2. Requestor/Agency ID	3. Agency Name	
---------------------	------------------------	----------------	--

II. Applicant Information: Type or clearly print answers in all fields before going to be fingerprinted.

1a. Last Name	1b. First Name	1c. Middle Initial	1d. Suffix
2. Any Alternative Names, Last Names, or Aliases		3. Social Security Number (Optional)	
4. Place of Birth (State or Country)	5. Date of Birth	6. Phone Number	7. Driver's License / State Identification Number
8. Issuing State			
9. Home Address		10. City	11. State
		12. ZIP Code	
13. Sex	14. Race	15. Height	16. Weight
		17. Eye Color	18. Hair Color

III. Livescan: Must be completed by the Livescan operator at the time of fingerprinting.
*After fingerprinting, the applicant shall return this signed and completed document to the requesting agency. The Livescan operator must return a completed copy of the form to the applicant.

1. Date Printed	Picture ID Type Presented	3. Transaction Control Number (TCN)	4. Livescan Operator
-----------------	---------------------------	-------------------------------------	----------------------

IV. Consent

I understand that my personal information, and biometric data being submitted by Livescan, will be used to search against identification records from both the Michigan State Police (MSP) and Federal Bureau of Investigation (FBI) for the purpose listed above. I hereby authorize the release of my personal information for such purposes and release of any records found to the authorized requesting agency listed above.

During the processing of this application, and for as long as my fingerprints and associated information/biometrics are retained at the State and/or FBI, they may be disclosed without my consent as permitted by MCL 28.248 and the Federal Privacy Act of 1974, 5 USC § 552a, for all applicable routine uses published by the FBI, including the Federal Register and for the routine uses for the FBI's Next Generation Identification.

Routine use includes, but is not limited to, disclosure to: governmental or authorized nongovernmental agencies responsible for employment, contracting, licensing, security clearances, and other suitable determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

Signature: _____ Date: _____

Procedure to obtain a change, correction, or update of identification records:

If, after reviewing his/her identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections, or updating of the alleged deficiency, he/she should make application directly to the agency which contributed the questioned information. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his/her record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which contributed the original information, the FBI CJIS Division will make any changes necessary in accordance with the information supplied by that agency. (28 CFR § 16.34)



Consent



Supporting Documentation

(4 of 4)



SAS Audit Criteria Continued:

- Applicant Appeal Process:
 - A formal appeal process for applicants wishing to challenge, correct, or update their criminal history record and is a two-part process.
 - Livescan RI-030 appeal language
 - {Agency} Appeal Process
- School agencies may share CHRI with an applicant for the purpose of challenge, correction, or update.
 - Prior to release, school agencies shall determine through picture ID that applicant and record (CHRI response) are “one in the same.”
 - Can include the state and federal portion of CHRI per recent clarification from the FBI.

A template has been created and available for the agency's use.

www.michigan.gov/cjicats (Template)



LIVESCAN FINGERPRINT REQUEST FORM RI-030



Appeal Part 1



III. Livescan: Must be completed by the Livescan operator at the time of fingerprinting. <small>*After fingerprinting, the applicant shall return this signed and completed document to the requesting agency. The Livescan operator must return a completed copy of the form to the applicant.</small>			
1. Date Printed	Picture ID Type Presented	3. Transaction Control Number (TCN)	4. Livescan Operator
IV. Consent			
<p>I understand that my personal information, and biometric data being submitted by Livescan, will be used to search against identification records from both the Michigan State Police (MSP) and Federal Bureau of Investigation (FBI) for the purpose listed above. I hereby authorize the release of my personal information for such purposes and release of any records found to the authorized requesting agency listed above.</p> <p>During the processing of this application, and for as long as my fingerprints and associated information/biometrics are retained at the State and/or FBI, they may be disclosed without my consent as permitted by MCL 28.248 and the Federal Privacy Act of 1974, 5 USC § 552a, for all applicable routine uses published by the FBI, including the Federal Register and for the routine uses for the FBI's Next Generation Identification.</p> <p>Routine use includes, but is not limited to, disclosure to: governmental or authorized nongovernmental agencies responsible for employment, contracting, licensing, security clearances, and other suitable determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.</p>			
Signature: _____		Date: _____	

Procedure to obtain a change, correction, or update of identification records:

If, after reviewing his/her identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections, or updating of the alleged deficiency, he/she should make application directly to the agency which contributed the questioned information. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his/her record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which contributed the original information, the FBI CJIS Division will make any changes necessary in accordance with the information supplied by that agency. (28 CFR § 16.34)

Appeal Part 2



[AGENCY NAME]

APPEAL PROCESS

for

Criminal History Record Information Challenge or Correction

Pursuant to federal statute, an individual may challenge the accuracy or completeness of any entry on his or her Criminal History Record Information (CHRI) response returned. Applicants wishing to challenge or correct his or her record must:

- Request an appointment with the [Hiring Personnel Title] within [Amount of Days] of having my CHRI response reported to me, if not proclaimed at the time of denial.
- Be given [Amount of Days] to rectify any questioned information within his or her record.

[Agency Name] will provide you with a copy of your CHRI response upon request. Wherein, you will need to make contact directly to the agency which contributed to the information in question. You can identify as to who the contributing agency is as it will be identified in your CHRI response.

Any challenge or correction progress conducted beyond the allotted time frame provided will only be considered at the discretion of [Agency Name].

If you are unable to resolve the information in question through this method, you may contact for an:

Out of State Record

Contact directly and make application to the FBI Criminal Justice Information Services (CJIS) Division, Attn: SCU, Mod. D2 1000 Custer Hollow Road, Clarksburg, WV 26306. Visit the FBI Website for more details, <http://www.fbi.gov/about-us/cjis/identity-history-summary-checks/or-der>.

In State Record

Contact directly the Michigan State Police at (517) 241-0606 or by e-mail at MSP-CRD-APPLHELP@michigan.gov. Please provide your name, method of contact, and reason behind your challenge or correction request (in detail).

As the applicant wishing to challenge or correct your record, it is your responsibility to keep [Agency Name] informed of any progress during this process.

Upon successful completion of a challenge or correction, the applicant may request from the Michigan State Police, Criminal History help desk, (517) 241-0606 his or her updated record to be forwarded to [Agency Name].

I, [Applicant Name] understand and agree to the terms and conditions set forth. I will work diligently to resolve any questioned information of my CHRI response and report back immediately to [Agency Name]. I further acknowledge that I received a copy of [Agency Name] Appeal Process and a copy of my CHRI response (if requested).

Signature _____

Date _____



Auditable Areas



- Reviewing:
 - Supporting Documentation
 - User Agreements
 - Local Agency Security Officer (LASO)
 - Personnel Security
 - Media Protection
 - Controlled Area
 - Incident Response
 - Secondary Dissemination
 - Security Awareness Training (SAT)



Questions?



MSP and NCJA User Agreement (5.1)



NCJAs receiving CHRI from the MSP *shall* complete a NCJA User Agreement for the Use of CHRI, RI-087 form.

This formal agreement specifies how the exchange of CHRI is to be conducted between the MSP and the NCJA through applicable security and management controls. The user agreement outlines each party's individual roles and responsibilities as it pertains to the day-to-day receipt and processing of CHRI and all that entails, including data ownership. The MSP and NCJA user agreements require the authorized signature of the agency representative (an employee of the agency with explicit authority to commit the agency to the agreement requirements) and the CJIS Security Officer of the MSP.



MSP and NCJA User Agreement

RI-087



RI-087 (07/2012)
MICHIGAN STATE POLICE
Criminal Justice Information Center
Page 3 of 3

agencies are only required to report felonies and confinement.

- Before releasing information on individuals or the person in question must be afforded the opportunity to be heard.
- CHRI is constantly being updated as new agencies contribute information. The record released is current.
- Certain statutes allow for the suppression or redaction of information.
- The MSP-CJIC retains records for the State of Michigan through the Federal Bureau of Investigation, which is a normal part of the criminal background check.

This Agreement commences on the date the last signatory either party. This Agreement may be terminated soon after immediately upon violation of the terms of the Agreement.

NONCRIMINAL JUSTICE AGENCY

Signature of Agency Representative

Title

Print or Type Name

MICHIGAN DEPARTMENT OF STATE POLICE

Signature of CJIS Security Officer, Criminal Justice Information Center

Print or Type Name

Dawn Brinningstaub

The "Agency Representative" must have the authority to bind the agency, typically the head of the organization or the person who will be receiving the responses.

Submit completed Agreement via United States mail or email.

ATTENTION: Applicant Help

Michigan State Police
Criminal Justice Information Center
333 S. Grand Ave.
P.O. Box 30634
Lansing, Michigan 48909-0634

RI-087 (07/2012)
MICHIGAN STATE POLICE
Criminal Justice Information Center
Page 1 of 3

AUTHORITY: MCL 28.242;
COMPLIANCE: Voluntary, however failure to complete this Agreement will result in denial of request.

NONCRIMINAL JUSTICE AGENCY USER AGREEMENT FOR RELEASE OF CRIMINAL HISTORY RECORD INFORMATION

between the

MICHIGAN STATE POLICE CRIMINAL JUSTICE INFORMATION CENTER

This agency hereinafter shall be known as "MSP-CJIC"

and

Agency Name [REDACTED]	Agency ID (if issued) [REDACTED]	Government Agency <input type="checkbox"/> Yes <input type="checkbox"/> No
Address [REDACTED]		
City [REDACTED]	State [REDACTED]	ZIP Code [REDACTED]
Contact Name (First, Middle, Last, Suffix) and Title [REDACTED]		
Telephone Number () [REDACTED] - [REDACTED]	Fax () [REDACTED] - [REDACTED]	Email Address [REDACTED]
Email Address for criminal history responses, if different from contact email address [REDACTED]		

This agency hereinafter shall be known as "User"

I. PURPOSE

This User Agreement is used to provide criminal history record information (CHRI) to employers, licensing agencies, and other agencies needing fingerprint-based criminal background checks.

Fingerprint-based criminal background checks must be explicitly mandated or allowed by law. National background checks must be authorized by federal law or a state statute approved by the U.S. Attorney General. The applying User is seeking background checks for:



Description of background check purpose (if employment or licensing, description of job and customers/clients served)

[REDACTED]

If school, grades included

If private security, private detective, or burglar alarm company; LARA license number

[REDACTED]

Law requiring allowing background checks, if known

[REDACTED]

II. THE PARTIES AGREE AS FOLLOWS

The MSP-CJIC will:

- Provide criminal history record information (CHRI) in response to fingerprint-based background checks, subject to the User's consent to the appropriate agency that reviews criminal histories for the User.

if this Agreement is violated or if the User is suspected of violating

entified in this Agreement.

ules, procedures, and policies, including those adopted by the state (CJIS) Board and national CJIC Policy Council regarding the use and

ested.

al history record information received. This includes, but is not limited

ecurity Officer who is responsible for ensuring compliance with security reement.

h access to criminal history information are aware of rules and CHRI.

electronic copies of CHRI to authorized personnel. Physical copies rolled, secure environment such as a locked cabinet in a room not tors. Electronic copies shall be protected with at least 128-bit eral encryption standard is FIPS 140-2.

ity allowed by law and log any CHRI sharing (either sending or a, at a minimum, the date, sending and receiving agencies, record share CHRI, means of transmission, and person who disseminated.

security incidents such as the theft/loss of physical records or the tems.

Physical media should be cross-shredded at a minimum, and deleted and repeatedly over-written with random 0s and 1s.

h CHRI received at the state repository. If a person could be adversely t be given the opportunity to challenge and correct a record before it is

days. Once the minimum retention time period has passed, the records until they are no longer needed for administrative, legal, audit, is Freedom of Information Act requests or legal actions.

ts to assure compliance with this Agreement.

CRIMINAL HISTORY RECORD INFORMATION LIMITATIONS

record Information (CHRI) has the following limitations:

as follows:

nd crime class under which the person was arrested. The arrest data tory field of name, race, sex, and date of birth. All arrests are

Prosecutor.

of the case and the ultimate disposition of the case.

file, or other databases maintained by the MSP are not part of the CHR

Agreements may be forwarded to: MSP-NCJAAgreement@michigan.gov



Local Agency Security Officer (LASO) (3.2.9)



Designated by the NCJA:

- Identify who is accessing CHRI.
- Identify how the NCJA is connected to CHRI.
- Ensure security measures are in place and working.
- Support policy compliance and ensure the reporting of any CHRI incident to the MSP Information Security Officer (ISO).



NCJA LASO Appointment (3.2.9)



CJIS-015 (09/2014)
MICHIGAN STATE POLICE
Criminal Justice Information Center

NONCRIMINAL JUSTICE AGENCY LOCAL AGENCY SECURITY OFFICER APPOINTMENT

AUTHORITY: 1974 PA 163; MCL 28.215, E.R.O. No. 2008-2, MCL 28.162, and R 28.5201. **COMPLIANCE:** MANDATORY

All Noncriminal Justice Agencies (NCJA) that have access to Criminal History Record Information (CHRI), a subset of Criminal Justice Information, shall appoint a security point of contact known as a Local Agency Security Officer (LASO). The LASO can be, but is not required to be, the NCJA department head (e.g., superintendent, president, director, etc.).

A change in appointment of the LASO must be reported to the Michigan State Police, Criminal Justice Information Center. A change in LASO can be reported by returning this completed form through one of the preferred methods listed below.

Send Completed Form To: Michigan Department of State Police Criminal Justice Information Center ATTN: Security and Access Section P.O. Box 30634 Lansing, MI 48909-0634 OR: E-mail: MSP-CJIC-ATS@michigan.gov OR: Fax: (517) 241 - 0865		For Additional Information: FBI CJIS SECURITY POLICY	
		Questions / Comments: Phone: (517) 241 - 0621	
I. LASO Information			
Appointed LASO (First Name, Last Name, M.I.)		Agency Name	Agency ID
Agency Address		City	State MI
Work Phone Number		Fax Number	
Email Address			
II. Approval			
Printed Name of Agency Head and Title			Date

www.michigan.gov/cjicats (Forms)



Personnel Security (5.12)

(1 of 2)



Screening requirements are performed prior to any individual gaining access to CHRI to determine if access is appropriate, and dependent on how your agency maintains CHRI, can include directly employed IT personnel. NCJA's must have a written process in place for the following:

- Any individual with a felony conviction shall be denied access to CJI/CHRI.
- For a criminal record other than a felony, any individual with an arrest without conviction or an individual believed to be a fugitive shall have their record reviewed to determine if access to CJI/CHRI is appropriate.
- CJI/CHRI access will be discontinued for any individual who is subsequently arrested or convicted of a crime, and must be reported to the MSP before access may be reinstated.
- Restricting CHRI media access for contractors and/or vendors where CHRI is stored and/or processed unless escorted (physically or virtually) by an authorized personnel.



Personnel Security (5.12)

(2 of 2)



For authorized users with access to CHRI, the NCJA shall maintain written processes of the specific steps taken for the following:

- Written documentation addressing the “immediate” termination of individual CHRI access upon termination of employment.
- Written documentation that addresses the review of CHRI access authorizations upon individual reassignment or transfer.
- A formal sanctions process for personnel with access to CHRI failing to comply with agency established information security policies and procedures.

A NCJA Policy template is now available for agency’s use and can be found at the following link: www.michigan.gov/cjicats (Template).



Media Protection (5.8)



NCJAs shall have established policy and procedures for the appropriate: security, handling, transporting, and storing of CHRI media. Each NCJA shall establish the following:

- An overall digital/physical media protection policy.
- Procedures restricting access to authorized user/personnel. Management controls are to exist for the processing and retention of CHRI media and for media to be secured in a controlled area.
- Procedures for transporting CHRI media from its original secured location to another. The steps taken to protect and prevent the compromise of the data in transit.
- Procedures for the appropriate disposal and sanitization of CHRI media when no longer needed, and the specific steps taken to protect and prevent CHRI media during the destruction process. All destruction is to be logged or documented.



Physical Protection (5.9)



NCJAs shall establish and implement physical protection policy procedures to ensure CHRI and information systems are physically protected through access control measures. When an agency cannot meet all the control requirements for a physically secure location, the agency shall review and adhere to 5.9.2- Controlled Area, which states the following:

- Limit access in controlled area during CJI/CHRI processing times.
- CHRI room or storage area should be locked at all times when not in use.
- Position CHRI to prevent unauthorized individuals from access and view.
- Agencies shall abide and carry out encryption requirements for digital storage of CHRI. (FIPS 140-2)



Questions?



Incident Response (5.3)

(1 of 2)



Each NCJA shall establish operational incident handling policy and procedure for instances of an information security incident of physical/digital CHRI media. Agencies are to ensure general incident response roles and responsibilities are included within the agency established and administered Security Awareness Training (SAT). Each NCJA shall establish:

- Information security reporting procedures outlining who to report to and how reporting happens through the agency chain of command upon discovery of any information security incident pertaining to CHRI.
- Incident handling capability procedures that includes adequate preparation, detection, and analysis, containment, eradication, recovery, and user response activities.



Incident Response (5.3)

(1 of 2)



Electronic and Physical Incident Handling Capability Procedures include:

- Preparation—firewalls, virus detection, malware/spyware detection, security personnel, and locked doors to prevent unauthorized access.
- Detection—monitoring preparation mechanisms for intrusions such as: spyware, worms, and unusual or unauthorized activities, etc. Can include building alarms and video surveillance.
- Analysis—identify how an incident occurred and what systems or CHRI media were compromised.
- Containment—security tools utilized or an agency plan to stop the spread of the intrusion.
- Eradication—removal plan of the intrusion before the system is restored and steps taken to prevent reoccurrence.
- Recovery—the ability to restore missing files or documents.



Incident Response (5.3)

(2 of 2)



Each NCJA shall establish:

- Procedures for the appropriate collection of evidence of an information security breach that meets relevant jurisdiction(s) for a CHRI security incident involving legal action (either civil or criminal) against a person or agency (calling law enforcement or contacting legal counsel).
- Procedures to track, document, and report information security incidents. An "Information Security Officer (ISO) Computer Security Incident Response Capability Reporting," form (CJIS-016) has been established, and is the required method of reporting security incidents to the MSP.

A NCJA Policy template is now available for agency's use and can be found at the following link: www.michigan.gov/cjicats (Template).



Information Security Officer (ISO) Computer Security Incident Response Capability Reporting CJIS-016



CJIS - 016 (09/2014)
MICHIGAN STATE POLICE
Criminal Justice Information Center
Page 2 of 2

2. What applications, systems and/or data were accessed? Did access include any personally identifying information or criminal justice information? Provide a description / list as to who you believe is affected or vulnerable to a similar incident.
3. When did the incident occur? Identify the time-frame and the operational phase (i.e., Was this a one-time occurrence or could certain events trigger it?)
4. Why did this incident happen? What allowed this incident to occur? Were there policies in place which may be applicable to controls in place which may help to prevent this type of incident from reoccurring?
5. What are the vulnerabilities and impacts associated with this incident? Describe what you believe are the vulnerabilities and systems as a result of this incident.

CJIS - 016 (09/2014)
MICHIGAN STATE POLICE
Criminal Justice Information Center
Page 1 of 2

INFORMATION SECURITY OFFICER (ISO) COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY REPORTING

AUTHORITY: MCL 28.215, MCL 28.162, and R 28.5201 COMPLIANCE: Mandatory; PENALTY: Loss of access to criminal justice information systems

Agencies shall promptly report criminal justice information system incidents to the Criminal Justice Information System (CJIS) Agency ISO in compliance with the FBI CJIS Security Policy. If a question does NOT apply, enter "N/A" to signify not applicable.

Send Completed Hard-Copy Form To: Michigan Department of State Police Criminal Justice Information Center ATTN: Information Security Officer P.O. Box 30634 Lansing, MI 48909-0634		For Additional Information: FBI CJIS SECURITY POLICY Questions / Comments: Phone: (517) 241 - 0807	
I. Agency Information			
Point(s) of Contact (First Name, Last Name, M.I.)		Agency Name	Agency ID
Agency Address		City	State <input type="text"/> Zip Code
Work Phone Number		Email Address	
Date of Report		Date of Incident	
II. Incident Information			
Location(s) of Incident:			
System(s) and/or Data Affected (e.g., CAD, RMS, File Server, etc.):			
Method of Detection:			
Nature of Incident:			
Incident Description:			
Actions Taken / Resolution:			
III. Incident Report			
1. How was the incident discovered? (e.g. via an audit trail, or accidental discovery)			



Secondary Dissemination (5.1.3)

(1 of 2)



Any disseminations of CHRI conducted outside of primary information exchange agreements are to be logged, including:

- The date record was shared
- Who made the request (Requesting Agency and Recipient Name)
- Whose record is being shared
- Who sent the shared copy (personnel)
- How the request was fulfilled

A Secondary Dissemination template has been created and is available for agency's use at: www.michigan.gov/cjicats
(Template)



Secondary Dissemination (5.1.3)

(2 of 2)



Dissemination Criteria:

A CHRI response may be shared with authorized user/personnel for a Michigan K-12 school so long as the individual remains employed with no separation from service by any school.

- K-12 schools can share with other K-12 schools, whether private or public, per MCL 380.1230a (11) & (12).
- K-12 schools cannot share responses with private entities (Contractors).
- K-12 schools may only share responses with Colleges/Universities, when identified as the authorized user/personnel, on behalf of a Public School Academy.



Security Awareness Training (SAT) (5.2)



Each NCJA shall have an established baseline SAT program for all personnel with access to CHRI provided by the agency within six months of assignment and every two years thereafter. At a minimum, for NCJAs that do not store CHRI digitally, SAT is to include:

- 5.2.1.1 Level One SAT:
 - Describes the topics required for all personnel who have unescorted access to CHRI.
- 5.2.1.2 Level Two SAT:
 - Describes the topics required for all personnel that have access to CHRI.

NCJAs storing CHRI digitally will be required to comply with SAT levels Three and Four as prescribed in the FBI CJIS Security Policy.

A SAT “fill-in” template has been created and is available for agency's use at: www.michigan.gov/cjicats (Template)



Additional Guidance: Digital CHRI

(1 of 2)



Digital Storage:

When an NCJA creates a digital copy of CHRI (e.g: saving a digital record from another original digital record, scanning a document, or creation of a spreadsheet) and subsequently stores this static CHRI, the following may also be applicable:

- 5.4–Auditing and Accountability of Information Systems
- 5.5–Access Control including: Account Management, Access Enforcement, Least Privilege, System Access Control, Access Control Criteria, Access Control Mechanisms, Unsuccessful Login Attempts, System Use Notification, Session Lock, Remote Access, and Personally-Owned Information Systems
- 5.6–Identification and Authentication: Advanced Authentication (AA)
- 5.7–Configuration Management: Access Restrictions for Changes, Least Functionality, Network Diagram, and Security of Configuration Documentation



Additional Guidance: Digital CHRI

(2 of 2)



Digital Storage Continued:

- 5.10—System and Communications Protection and Information Integrity, including: Boundary Protection, Encryption, Partitioning and Virtualization, and Patch Management.

And if you are using a mobile device such as a laptop, tablet, or smartphone you must *also consider the following*:

- 5.13—Mobile Devices including: Wireless Protocols, Cellular Devices, Cellular Service Abroad, Bluetooth, Mobile Hotspots, Mobile Device Management (MDM), Wireless Device Risk Mitigations, System Integrity, Patching/Updates, Malicious Code Protection, Mobile Incident Response, Access Control, Identification and Authentication, Local Device Authentication, Advanced Authentication (AA), and Compensating Controls.



Compliance Audit Closing



Once a Compliance Audit Review is completed your agency will have a better understanding of necessary practices, policies, and procedures. What to expect following the audit review:

- A draft compliance audit report will be created and sent to your agency approximately (15) business days from the date of your audit.
- Your agency will be asked to respond within (30) days, in regards to your school's corrective actions in response to any Out of Compliance area(s).
- At the end of (30) business days, whether we've received your agency's response or not, the MSP will provide a final draft indicating whether your audit compliance is complete and will include additional corrective actions.

Upcoming compliance cycle changes:

- Zero-cycle audits end September 30, 2017.
- CJIS System Officer (CSO) referrals begin.



Resources & Tools



Our website provides a one-stop shop for obtaining:

- Forms
- Guidance
- Training Information
- Templates
- Listserv Archives

MSP Security & Access Website:

www.michigan.gov/cjicats



THANK YOU !!!!!

For your time and attention.
We look forward to working with
you in the future...