Appropriate Use of Systems and Data

Version: 4/11/2025	Document Number: MNJIS-5000	Distribution: BCA

Policy Statement / Objective:

In support of criminal justice agencies and other authorized users, the Minnesota Bureau of Criminal Apprehension (BCA) operates a number of data repositories and a secure network. This system and various tools allow authorized users, both employees and contractors, to access data from state and federal sources in order to perform their official functions. Through Authorized Agencies, contractors may have access to the physical or logical spaces in which the secure network and data are held.

Authorized users are employed in either a criminal justice or non-criminal justice agency, while contractors may be a government entity, private business, agency, or individual that has entered into an agreement with the Authorized Agency.

In some instances, the statute that created the repository authorizes the access to and use of the data. In other instances, access to the data is governed by the provisions found in the Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13 and Minnesota Statutes, section 299C.46, as well as additional federal and state policies and laws.

Access to and use of the secure network and data must be done in compliance with MNJIS-5002 CJDN Security.

The purpose of this policy is to:

- Establish a working relationship between the BCA and authorized agencies that promotes and supports appropriate use at all times,
- Establish the standards and guidelines for appropriate use of the repositories and secure network,
- Document the processes used to determine if the use is inappropriate, and
- Provide penalties for failure to meet the standards outlined in this policy.

The BCA's goal is that Authorized Agencies, users, and contractors be in full compliance with all requirements. Agencies and users that fail to comply with this policy are subject to the sanctions described later.

This Policy and the appendix are periodically revised as issues and examples are identified. Notice is sent to agency heads regarding the availability of revised documents.

Definitions:

As used in this policy, the following terms have the meaning given.

Appropriate Use: The agency that employs the individual user is eligible under the applicable statutes and regulations to have access to the secure network and the data, and that the data have been retrieved as part of an employee's work assignment or are retrieved to share the data with another entity authorized by law to receive them. Appropriate use is further defined as a contractor's access to the physical or logical space that is required for the work being done by the contractor. See Minnesota Statutes, sections 13.05 and 13.055 and the FBI CJIS Security Policy. If an agency has a more restrictive policy on access and/or sharing, the employee or contractor must also follow the agency policy.

Authorized User: An individual user who is eligible under the applicable statutes and regulations to have access to the secure network and data for the purposes of their work assignment.

Authorized Agency: A criminal justice agency or noncriminal justice agency as defined in Minnesota Statutes, Section 299C.46.

Contractor: A private business, government entity, agency, or individual who has entered into an agreement for the administration of criminal justice or noncriminal justice functions with an Authorized Agency and have access to the physical or logical space in which the secure network and data are kept.

Follow-Up Audit: An audit of an agency following issues identified during a routine audit or when inappropriate use has been found, including from self-reporting. A follow up audit can occur anytime.

Hot File: A Minnesota or FBI data file containing information about persons or property that can be accessed by Authorized Agencies and their employees in performance of their authorized duties.

Inappropriate Use: Any use that is not "appropriate use" or for which there is no acceptable lawful explanation or of documentation why the transaction was conducted. Examples of a lawful explanation include "assigned to traffic enforcement", "assigned to Safe and Sober campaign", or "to determine eligibility for benefits from a noncriminal justice agency".

Intentional: When an employee or contractor knowingly behaves in a manner that is inappropriate or repeats a behavior after being informed that the behavior is not acceptable. Determining the intent of the employee or contractor is done by the agency.

Non-Compliant: An agency has not taken the necessary steps to conduct the investigation or to resolve the issues identified during an audit, follow up audit, or investigation.

Unintentional: When an employee or contractor unknowingly behaves in a way that results in inappropriate use.

Policy:

I. Access and Control

Access to and use of data in BCA repositories or available from other repositories via the secure network is controlled by one or more of the following:

A. A specific state statute – e.g. Minnesota Statutes, section 299C.40 controls the Law Enforcement Incident Search or LEIS (formerly known as the Comprehensive Incident-Based Reporting System or CIBRS).
B. Minnesota Statutes, section 299C.46 controls the use of the secure network.
C. Federal regulations implemented through the FBI CJIS Security Policy.
D. Federal regulations implemented for data files including, but not limited to, N-DEx (National Data Exchange) and the NICS Indices (National Instant Criminal Background Check System).
E. The Rules of Public Access to Records of the Judicial Branch control access to court case information.
F. Policies adopted by other agencies concerning access to and use of that agency's data–e.g. Corrections' policies on access to the Statewide Supervision System (S^3).
G. Terms of the contract between the agency and the BCA

H. The Bureau of Criminal Apprehension, MNJIS-5002 CJDN Security.

A chart showing all of the repositories or tools with authorized users and examples of appropriate and inappropriate use is attached as Appendix 1.

It is never appropriate to retrieve data on yourself. Data practices procedures must be used to obtain data on you. There are test records available on the BCA LaunchPad for use in understanding how a particular repository works.

II. Determination of Appropriate Access

A. The primary tool used by the BCA to determine inappropriate use is the agency audit. See Audit Policy MNJIS-5005. Transactions involving Minnesota and federal criminal history and "Hot File" data are audited every three years as required by the FBI. Additional audits are performed for agencies:
1. with access to Law Enforcement Incident Search (LEIS) (formerly known as CIBRS);
2. with access to National Data Exchange (N-DEx);
3. with access to Gun Permit Background Check (GPBC);
4. that are Integrated Search Services users who access the S^3; and
5. that submit fingerprint-based background check requests as authorized under state and federal law.

B. Use is reviewed at both an individual user and agency level. If issues are identified during an audit, the agency's Trainer/Auditor will explain the next steps. See Audit Policy MNJIS-5005. Inappropriate use may also be identified through a variety of means, including, but not limited to:
1. as a result of a question asked by an agency user.
2. in response to an official agency request.
3. following allegations of inappropriate use by an authorized user or agency.
4. analysis of system use by the BCA.
5. based on transactions identified by the BCA's pattern analysis tool; or
6. self-reporting.

C. Examples of issues that can result in a finding of inappropriate use or noncompliance include, but are not limited to:
1. Unintentional inappropriate use of data retrieved from BCA repositories or repositories reached via the BCA secure network by either employees or contractors
2. Unintentional inappropriate use of or access to the secure network by either employees or contractors
3. Intentional inappropriate use of data retrieved from BCA repositories or repositories reached via the BCA secure network by either employees or contractors
4. Intentional inappropriate use of or access to the secure network by either employees or contractors
5. Retrieving data and providing it to an individual whose access to the system or network has been suspended by either employees or contractors
6. Failure to ensure the security of the data and equipment used to retrieve the data by either employees or contractors
7. Retrieval or sharing of data in a manner not authorized by the governing statute or federal regulation by either employees or contractors
8. Failure to investigate allegations of inappropriate use presented by BCA to the

agency

9. Failure to respond to BCA requests for information about transactions performed by agency users; or
10. Failure to address problems found during an audit or follow-up audit

D. If the agency is in litigation about the transactions, it must let the CJIS Systems Officer (CSO) at the BCA know that fact. Once there is an agreement to settle the case or a verdict is given, the agency must report to the BCA on the appropriateness of the query.

III. Sanctions

In addition to any employment consequences for behavior found to be in violation of this Policy, there may be additional consequences imposed by the BCA that affect the Authorized Agency or Authorized User's ability to use systems and tools provided by the BCA. Any consequences imposed by the BCA are based upon the investigation and determination of inappropriate use by the Authorized Agency.

The BCA recognizes that an Authorized Agency has a separate human resources process that it must follow when there is a complaint against one of the agency's Authorized Users. The BCA also knows that there may be a collective bargaining agreement that directs which processes must be used in the investigation and evaluation of a complaint. As Minnesota Statutes, Section 13.43 classifies data about alleged misconduct by an Authorized User as private data, the agency head should consult with the CJIS Systems Officer (CSO) prior to finalizing any disciplinary decisions so that the consequences related to data or system access can be coordinated. The CJIS Systems Officer (CSO) will have an opportunity to evaluate the general circumstances and determine if additional sanctions, related only to system access, will be imposed by the BCA. Any data shared by the agency are documented in the BCA case management system and are classified in the same way as in the Authorized Agency. See Minnesota Statutes, Section 13.03, Subd. 4.

The BCA further recognizes that an Authorized Agency has a separate procurement process by which contractors are selected and agreements on duties are reached as well as how complaints against contractors are handled.

A. Criteria Used to Determine Sanctions

The criteria to be used in determining sanctions include, but are not limited to the following:

1. How many transactions were found to be inappropriate?
2. Over what period of time did the transactions occur?
3. What types of transactions were inappropriate?
4. What was the purpose of the inappropriate use?
5. Was the inappropriate use intentional or unintentional?
6. How much experience does the Authorized User or contractor have?
7. How much training does the Authorized User or contractor have and what type?
8. Is there a history of inappropriate use?
9. If there is a history of inappropriate use, what were the prior corrective actions taken?
10. Was the criminal justice information re-disseminated? If yes, to whom?
11. Has the Authorized User or contractor taken responsibility for the conduct?
12. Is there a history of inappropriate use at the Authorized Agency?
13. What steps has the Authorized Agency taken to address the inappropriate use?

B. The determination whether there will be any BCA- imposed sanctions is made by the CJIS Systems Officer (CSO) in consultation with the Senior Legal Analyst for MNJIS. This evaluation is based solely on information provided to the BCA by the Authorized Agency and no independent investigation is done by the BCA.

C. Sanctions imposed on the Authorized Agency or Authorized User may include, but are not limited to, any of the following:

1. Requiring the Authorized User or contractor to be re-trained and re-take any certification testing applicable to the criminal justice information in question
2. Requiring that the Authorized User or contractor's transactions be monitored for a stated period of time to ensure transactions are appropriate
3. Loss of access to the system(s) or tool(s) where the inappropriate use occurred
4. Loss of access to other systems or tools the Authorized User is authorized to use
5. Loss of all access to BCA systems or tools for a period of time
6. Loss of all access to BCA systems or tools on a permanent basis
7. Requiring the Authorized User to notify any future employer of the inappropriate use
8. Requiring that any Authorized Agency that agrees to hire the Authorized User or contractor monitor the Authorized User or contractor's use of BCA systems or tools to ensure appropriate use

D. Within ten (10) days of the Authorized Agency determining an Authorized User or contractor's use of or access to the secure network or data was inappropriate, the Authorized Agency shall inform the BCA of the determination.

E. If a contractor fails to use their access to the physical or logical space appropriately, sanctions may be placed upon the Authorized Agency. The Authorized Agency is solely responsible for any and all of their contractor's inappropriate use.

F. Within 30 days of the receipt of the notice described in Section D, the BCA will make a decision as to the imposition of sanctions and will notify the affected party and agency in writing. The affected party will be given ten (10) business days to make a written appeal to the BCA's Superintendent and the Deputy Superintendent for Minnesota Justice Information Services. Any appeal to the BCA would apply solely to the sanction and not to the determination of misuse as no independent determination is made by the BCA. The affected Authorized User may ask the agency, with whom they contract or are employed by, to make an appeal on their behalf. The agency must document the affected Authorized User's or contractor's request in the appeal. The appeal should include information about the sanction imposed that the affected Authorized User wants reconsidered. The Superintendent and Deputy Superintendent may request a meeting with the affected party if they wish more information or clarification. The meeting may be held in-person or via an interactive method where all parties can be seen as well as heard.

G. The Superintendent and Deputy Superintendent will have ten (10) business days from receipt of the appeal or the meeting to issue a written decision about the issues raised by the appeal. A copy of the decision will be provided to the affected party and employing agency.

Roles and Responsibilities:

The BCA provides training on appropriate use of the various repositories and in some instances requires that users be certified to have access. Some of the systems that require certification also require recertification. The BCA enforces all certification and recertification requirements. The agency head is responsible for ensuring that Authorized Users and contractors review relevant training for use of the secure network and accessing the repositories as well as completing certification when required.

All personnel accessing the Criminal Justice Data Network (CJDN) and personnel who have access to criminal justice information must:
1. Complete appropriate Awareness & Training, and
2. Recertify Awareness & Training annually

To ensure that all authorized agencies and users are in compliance with the applicable requirements, the BCA has a Training and Auditing Unit whose staff members are responsible for assisting agencies and their users as well as auditing transactions for compliance.

References:

1. BCA MNJIS-5002 CJDN Security
2. BCA MNJIS-5005 FBI CJIS Audits, Audit Compliance, And Audit Sanctions
3. FBI CJIS National Data Exchange (N-DEx) Policy and Operating Manual
4. BCA CJIS LaunchPad

Appendix 1: A Summary of Appropriate Use by System/Tool

Note: This table is a summary and is not intended to cover all situations.

Automated Fingerprint Identification System contains biometrics and data for persons arrested or booked for an offense, persons who are incarcerated and/or subject to supervision by correctional institutions or probation authorities, persons registered as predatory offenders, and persons whose fingerprints were found at crime scenes.	
Abbreviation	AFIS
Citation	13.87, Subd. 1(b), 299C.09, 299C.10, 299C.11
Users *Who Can Query*	Latent fingerprint examiners at certain law enforcement agencies.
Access Rules	Access granted via an approved agency following training provided by the BCA.
Appropriate Use	Appropriate use means the agency that employs the individual user is eligible under the applicable statutes and regulations to have access to the secure network and the data, and that the data have been retrieved as part of an employee's work assignment or are retrieved to share the data with another entity authorized by law to receive them
Inappropriate Use - Examples; Not Conclusive	Any unauthorized access or dissemination of data

Automated License Plate Readers BCA created extract of data used to cross-check license plates captured by the reader.	
Abbreviation	ALPR

Citation	13.824, subd. 2(b);
	168.346;

	171.12;
	171.18;
	USC 2721

Users *Who Can Query*	Law enforcement
Access Rules	No training available
Appropriate Use	Locate stolen vehicles; find individuals with a warrant for their arrest; find a missing person; identify individuals with a suspended, revoked or cancelled driver's license; can be used for investigations when combined with license plates captured by the reader
Inappropriate Use - Examples; Not Conclusive	Any use not within the definition of "appropriate use"

Court Integration Services Minnesota Judicial Branch system that contains data from criminal court cases, juvenile delinquency cases and civil cases.	
Abbreviation	CIS
Citation	None
Users *Who Can Query*	As authorized by Courts
Access Rules	No training available
Appropriate Use	A legitimate business need defined by the Courts as follows: to meet a requirement, duty or obligation for the efficient performance of government tasks or governmental responsibility that is required or authorized by law or court rule in connection with a proceeding
Inappropriate Use - Examples; Not Conclusive	Retrieving data without a legitimate business need as defined by Courts

Criminal Gang Investigative Data System Database of individuals law enforcement agencies determine are or may be engaged in criminal gang activity.	
Abbreviation	Gang Pointer
Citation	299C.091
Users *Who Can Query*	Criminal justice agencies
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	Assist criminal justice agencies in the investigation and prosecution of criminal activity by gang members. To determine if an individual has met the statutory criteria for entry into the database. Review is required when issuing a permit to carry
Inappropriate Use - Examples; Not Conclusive	Any use unrelated to investigating and prosecuting known or suspected gang members

Criminal History System Minnesota criminal history information on individuals and system to allow agencies and others with authority to update or correct criminal history records.	
Abbreviation	CHS
Citation	13.87;

	299C.095;
	299C.111;
	299C.46

Users *Who Can Query*	Criminal justice and non-criminal justice agencies
Access Rules	Trained and certified before access and annually thereafter; training available online and in a classroom
Appropriate Use	Assist criminal justice agencies in investigating and prosecuting crime; providing corrections and supervision services; identify records in suspense; correct data in records and to resolve suspense status. Non-criminal justice agencies may use the information to determine eligibility for benefits or to disburse licenses
Inappropriate Use - Examples; Not Conclusive	Any unauthorized access or dissemination of data or use unrelated to an appropriate use

Crime Reporting System System to collect crime statistics to be reported to the FBI and for use in the MN Crime Book.	
Abbreviation	CRS
Citation	299C.05; 299C.22
Users *Who Can Query*	Law enforcement
Access Rules	Training available online and in a classroom
Appropriate Use	Enter crime statistics and provide supplemental reports to document criminal activity in Minnesota; obtain reports about statistics
Inappropriate Use - Examples; Not Conclusive	Any use not related to crime statistics

DVS Access Different functionality to access motor vehicle registration, driver's license & government identification data including photographs.	
Abbreviation	DVS Access

Citation	18 USC 2721;
	168.346;
	171.12

Users *Who Can Query*	Criminal & non-criminal justice agencies
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	For government entities to carry out functions required to be performed by law & in connection with any court proceedings
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose or function or a photograph for a reason not in the governing statute

Driver & Vehicle Services Databases holding motor vehicle registration, driver's license & government identification data.	
Abbreviation	DVS

Citation	18 USC 2721;
	168.346;

	171.12
Users *Who Can Query*	Criminal & non-criminal justice agencies
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	For government entities to carry out functions required to be performed by law & in connection with any court proceedings
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose or function

Driver License Photo Photographs associated with a driver's license or a government- issued identification card.	
Abbreviation	DVS
Citation	171.07, subd. 1a
Users *Who Can Query*	Criminal justice agencies; public defenders; medical examiners
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	To criminal justice agencies for the investigation and prosecution of crimes; serve process; enforce no contact orders; find missing person; investigate and prepare cases for criminal, juvenile and traffic court; supervise offenders; locate individuals required to register as a predatory offender; public defenders for investigation and case preparation; medical examiners to identify the deceased
Inappropriate Use - Examples; Not Conclusive	Retrieving a photo of a person for any reason not listed in the statute

DWI Dashboard	
Abbreviation	none
Citation	169.09, subd. 13
Users *Who Can Query*	Law enforcement
Access Rules	No training available
Appropriate Use	For law enforcement to evaluate where alcohol-related accidents and events are occurring to deploy resources to address issues
Inappropriate Use - Examples; Not Conclusive	Any use not related to reducing alcohol- related accidents and events

eCharging Electronic workflow of charging documents from law enforcement to prosecution to Courts; search warrants from law enforcement to Courts and DWI administrative forms to Driver and Vehicle Services	
Abbreviation	none
Citation	299C.41
Users *Who Can Query*	Law enforcement; prosecutors; courts
Access Rules	Training provided at implementation; on request by an agency and available online
Appropriate Use	For law enforcement to prepare a search warrant or prepare case for submission to the prosecutor; for the prosecutor to review the case and request more information or decline to charge or prepare complaint; for submission of citations

	electronically by law enforcement; submission of test results to DVS for implied consent; for Courts to review complaints or search warrants and either sign or reject them
Inappropriate Use - Examples; Not Conclusive	Using data without a work-related purpose

Gun Permit Background Check A system for use in conducting background checks for permits to carry and permits to purchase/transfer	
Abbreviation	GPBC
Citation	624.7131; 624.714
Users *Who Can Query*	Sheriffs and police departments
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	To process background checks either prior to permit issuance or required during the life of the permit
Inappropriate Use - Examples; Not Conclusive	Any use not related to conducting background checks for gun permits

Integrated Search Service An interface that allows a user to search multiple databases in one location	
Abbreviation	ISS
Citation	13.873
Users *Who Can Query*	Criminal justice agencies
Access Rules	Training available
Appropriate Use	For criminal justice agencies to more efficiently search multiple repositories to which they are authorized access; appropriateness of use is dependent on the rules governing the underlying source system
Inappropriate Use - Examples; Not Conclusive	Any use that is not within the definition of "appropriate use"

The International Justice and Public Safety Network Network for the exchange of law enforcement, criminal justice, and public safety- related information among state, local, tribal, and federal agencies with a law enforcement component.	
Abbreviation	Nlets
Citation	n/a
Users *Who Can Query*	Criminal Justice Agencies
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	For criminal justice agencies to exchange information between states, Canada and Mexico; Nlets has established restrictions based on file type
Inappropriate Use - Examples; Not Conclusive	Any use that is not within the restrictions established by Nlets

Interstate Identification Index Cooperative federal-state system for the exchange of criminal history records	

Abbreviation	III
Citation	28 CFR Part 20
Users *Who Can Query*	Criminal justice agencies
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	Criminal justice purposes including screening of applicants for employment in criminal justice agencies
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose

Keeping Our Police Safe A system to get messages to officers quickly before data for NCIC entry is completely compiled.	
Abbreviation	KOPS
Citation	None
Users *Who Can Query*	Law enforcement
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	Officer safety; safety of an individual; non- safety related officer alerts
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose

Law Enforcement Incident Search Statewide database of law enforcement incident data to be accessed via the Law Enforcement Message Switch.	
Abbreviation	LEIS
Citation	299C.40
Users *Who Can Query*	Specific MN law enforcement – see statute
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	Prepare a case against a person for the commission of a crime; serve process in a criminal case; inform law enforcement officers of safety risk before service of process; enforce no contact orders; locate missing persons; conduct background investigation on peace officers
Inappropriate Use - Examples; Not Conclusive	Gun permits checks; non-peace officer pre-employment background checks; provide data to law enforcement outside MN; MN law enforcement not trained and certified

Law Enforcement Message Switch A gateway to query multiple repositories including CHS, Gang Pointer, DVS, DL Photo, III, KOPS, LEIS, MRAP, NCIC, NICS, PTS, POR, Warrants, OFPs, DANCOs, and HROs	
Abbreviation	LEMS (Portals)
Citation	None
Users *Who Can Query*	Criminal and non-criminal justice agencies
Access Rules	Trained and certified before access and annually thereafter
Appropriate Use	Access is controlled by agency role and authority; appropriate access is dependent on the rules governing the underlying source system

Inappropriate Use - Examples; Not Conclusive	Any use that is not within the definition of "appropriate use"

Livescan Message Enhancement Provides summary data from criminal bookings, response data from the BCA, and metrics about employees performing booking and fingerprint collection.	
Abbreviation	LME
Citation	13.43, subd. 2 and 4; 13.87
Users *Who Can Query*	Law enforcement agencies who perform bookings and collect fingerprints and palm prints
Access Rules	Training not available
Appropriate Use	Resolve issues with booking data or fingerprints or palm prints
Inappropriate Use - Examples; Not Conclusive	Any use that is not within the definition of “appropriate use”

Minnesota Repository of Arrest Photographs Central repository of booking and arrest photos	
Abbreviation	MRAP
Citation	13.87; 299C.46
Users *Who Can Query*	Criminal justice agencies
Access Rules	No training available. User manual is available in the application.
Appropriate Use	Case preparation and investigation
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose

Minnesota Warrants File Warrants for the arrest of individuals	
Abbreviation	None
Citation	13.82, subd. 19
Users *Who Can Query*	Law enforcement, corrections, probation
Access Rules	Trained and certified before access and annually thereafter; training available online and in a classroom
Appropriate Use	Determine if there is an open warrant for an individual's arrest
Inappropriate Use - Examples; Not Conclusive	Any use unrelated to determining if a warrant exists

National Crime Information Center - Restricted files* Computerized information system authorized to link local, state, tribal, federal, foreign and international criminal justice agencies to exchange information	
Abbreviation	NCIC
Citation	28 CFR Part 20
Users *Who Can Query*	Criminal justice agencies; non- criminal justice agencies with specific authority
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	For a criminal justice purpose including screening of applicants

	for employment. For purposes of screening an individual as provided by law by a non-criminal justice agency.
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose

National Crime Information Center - Unrestricted Files** Computerized information system authorized to link local, state, tribal, federal, foreign and international criminal justice agencies to exchange information	
Abbreviation	NCIC
Citation	28 CFR Part 20
Users *Who Can Query*	Criminal justice agencies; non- criminal justice agencies with specific authority
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	For a purpose consistent with the agency's responsibilities. For purposes of screening an individual as provided by law by a non-criminal justice agency.
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose

National Data Exchange The N-DEx system provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries.	
Abbreviation	N-DEx
Citation	CJIS N-DEx Policy and Operating Manual
Users *Who Can Query*	Law enforcement agencies, prosecutors, pretrial service and release agencies.
Access Rules	Section 1.3.3 of policy delineates 11 authorized agencies who can access. Section 2.4.3 of policy delineates requisite training. Trained and certified before access and annually thereafter
Appropriate Use	Gather data for the following investigations; law enforcement cases, pretrial release, intake assessments, correctional institution purposes, criminal justice employment background checks, training, NICS related checks, pre-sentence, supervision purposes
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work- related purpose, any use not related to the authorized investigations. Training purposes must not include curiosity searches, browsing or self- queries.

National Instant Criminal Background Check System Indices Database with information about persons prohibited under federal law from receiving or possessing a firearm.	
Abbreviation	NICS
Citation	28 CFR Part 25
Users *Who Can Query*	Law enforcement
Access Rules	Training available for data entry into NICS. Trained and certified before access and annually thereafter; training available online
Appropriate Use	Gather information to determine if an individual is disqualified

	from receiving a permit to purchase/transfer or a permit to carry; have an explosives permit or license; enter records into NICS; sheriffs can use for annual check of carry permit holders and for renewal of carry permits
Inappropriate Use - Examples; Not Conclusive	Any use not related to processing permit applications, renewals and annual checks of permit to carry holders; explosives permits or entry into NICS

Permit Tracking System Database of persons authorized to carry pistols, denied applications and revoked permits	
Abbreviation	PTS
Citation	624.714
Users *Who Can Query*	Prosecutors, law enforcement
Access Rules	Training provided by MN Sheriffs Association. User Guide in the application.
Appropriate Use	Sheriffs: manage permit to carry applications; denials, renewals and annual checks & revocations; police & prosecutors to verify permit
Inappropriate Use - Examples; Not Conclusive	Any use unrelated to permit to carry processing, permit renewal or annual check; or permit verification

Predatory Offender Registry Central repository of information on predatory offenders who are required to register	
Abbreviation	POR
Citation	243.166; 299C.093
Users *Who Can Query*	Law enforcement; corrections; certain parts of MN DHS (State Operated Services and Background Studies under 245C); to child protection workers in certain circumstances
Access Rules	Trained and certified before access and annually thereafter; training available online and in a classroom
Appropriate Use	Investigate cases; supervise predatory offenders; at MN Sex Offender Program for purposes in section 246.13, subd. 2(b); at MNDHS Licensing for background studies; to child protection for family assessment
Inappropriate Use - Examples; Not Conclusive	Any use not related to supervision of offenders or investigating a crime; duties of personnel related to individuals civilly committed as sexually dangerous persons or sexually psychopathic personalities; or conducting background studies under Chapter 245C; looking up tenants for housing in a community; child protection for family assessments

PrintPrint An archive of all Livescan transmissions that allows review of fingerprint submissions, ability to print copies of a fingerprint card, and access to view and print the FBI's master fingerprint card for any record in their files.	
Abbreviation	PrintPrint
Citation	13.43, subd. 2 and 4; 13.87

Users *Who Can Query*	Local agency law enforcement users who need to access and print archived prints or who do not have Livescan printers.
Access Rules	Trained and certified before access and annually thereafter; training available online
Appropriate Use	Review of fingerprint submissions, copies of fingerprint cards, and access to the FBI’s master fingerprint card.
Inappropriate Use - Examples; Not Conclusive	Any use that is not within the definition of “appropriate use”

Statewide Supervision System Department of Corrections system with information on offenders under supervision pre- or post-trial, or in detention	
Abbreviation	S^3
Citation	241.065
Users *Who Can Query*	Criminal justice agencies as defined in 13.02; MN Sex Offender Program; public defenders
Access Rules	No training available
Appropriate Use	Monitoring and enforcing conditions of release; investigative tool for criminal justice agencies for criminal justice purposes only; public defender access limited to preparation of a criminal case; DHS use limited to treatment facility staff, special review board members and end-of-confinement review committee members; MSOP use is for management of current patients
Inappropriate Use - Examples; Not Conclusive	Retrieving data on a person without a work-related purpose.

* NCIC Restricted files: Gang, Known or Appropriately Suspected Terrorist, Supervised Release, National Sex Offender Registry, Protection Order Files, Identity Theft, Protective Interest, Person with Information data in Missing Person files, Violent Person Files and NICS Denied Transactions File

** NCIC Unrestricted files: Article; Boat; Foreign Fugitive; Gun; Image; License Plate; Originating Agency Identifier; Immigration Violator; Securities; Supervised Release; Unidentified Person; Vehicle/Boat Part; Vehicle; Wanted Person

Revision History:

Previous Version: 06/11/2020

Description of Changes:

- Added Awareness & Training verbiage to Roles and Responsibilities section
- Fixed links in References section
- Updated Access Rules in Appendix I for the following entries: Criminal Gang Investigative Data System, CHS, DVS Access, Driver & Vehicle Services, Driver License Photo, Gun Permit Background Check, The International Justice and Public Safety Network, Interstate Identification Index, Keeping Our Police Safe, Law Enforcement Incident Search, Law Enforcement Message Switch, Minnesota Warrants File (previously ‘Warrants Index of Minnesota’), NCIC Restricted Files, NCIC Unrestricted Files, National Data Exchange, National Instant Criminal Background Check System Indices, Predatory Offender Registry, and PrintPrint
- Added links for Policies, Statutes, etc. where appropriate

- Added Revision History and Document Archival sections
- General cleanup (grammar, punctuation, formatting, etc.)

Document Archival:

Reason for Archival:

Initials and Date	*Title*