141. ACCESS AND USE OF THE COMPREHENSIVE INCIDENT BASED REPORTING SYSTEM (CIBRS) DATABASE SYSTEM

RICHFIELD POLICE DEPARTMENT POLICY

Effective Date:	12/05/12
No. of Pages:	6
Serial Number:	10-041
Authority:	Chief Jay Henthorne

NOTE: This policy is for internal use only and does not enlarge an employee's civil or criminal liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this policy, if proven, can only form the basis of a complaint by this Department, and then only in a non-judicial administrative setting.

I. PURPOSE

The purpose of this policy is to comply with MSS 29C.40 as well as rules and policies prescribed by the Minnesota Department of Public Safety, Bureau of Criminal Apprehension (BCA), regarding the access and the use of the CIBRS database system.

II. POLICY

This policy shall be considered the official CIBRS Policy for the Richfield Police Department, regarding the operation of the CIBRS system. All staff must follow the policies contained herein. This will assure proper usage of the system and adherence to all local, state, and federal regulations that govern the use of the MNJIS computer system.

III. DEFINITIONS

AUDIT: A process conducted by staff of the Minnesota Department of Public Safety, Bureau of Criminal Apprehension whereby the Agency is assessed on their compliance with the rules specified in the user agreement.

CIBRS: The Comprehensive Incident Based Reporting System, a statewide repository of incident based data from the Minnesota law enforcement agencies. This electronic data sharing program is designed to provide law enforcement access to data submitted by agencies, on a statewide level. The data is recorded by the local agency within their records management system. The data is owned and maintained by the local agency; however data that is public at the local agency will change to private data in CIBRS.

CIBRS TRAINING CERTIFICATION: Members of the Richfield Police Department authorized to access the CIBRS system will meet the training and certification requirements as prescribed in the use agreement and the CIBRS policy of the Minnesota Department of Public Safety.

Initial Certification: The BCA training program and successful completion of the examination.

Recertification: An examination which must be successfully completed every two years.

CONFIDENTIAL DATA OF INDIVIDUALS: As defined in MS 13.63, Subdivision 3, confidential data on individuals means the data which is made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of the data.

GOVERNMENT ISSUED PHOTO ID: This includes a state issued driver's license or ID card, a certified passport, or military ID card issued by a recognized branch of the United States military.

NON-PUBLIC DATA: As defined in MSS 13.02, Subdivision 9, non-public data means data not on individuals that is made by statute or federal law applicable to the data: (a) not accessible to the public and (b) accessible to the subject, if any of the data.

PRIVATE DATA ON INDIVIDUALS: As defined in MSS 13.02, Subdivision 12, private data on individuals means data which is made by statute and or federal law applicable to the data: (a) not public, and (b) accessible to the subject, of the data.

PROTECTED NON-PUBLIC DATA: As defined in MSS 13.02, Subdivision 13, protected non-public data means data not on individuals which is made by statute or federal law applicable to the data (a) not public and (b) not accessible to the subject of the data.

RESPONSIBLE AGENCY: An agency that is responsible for the completeness and accuracy of a data record within the CIBRS system.

SUBMITTING AGENCY: The entity responsible for ensuring the successful submission of the law enforcement agency's records to the CIBRS database.

USER AGREEMENT: A document entered into by the Minnesota Department of Public Safety and the Richfield Police Department which list the requirements and responsibilities to be met by both entities

IV. PROCEDURE

ACCESS CIBRS BY DEPARTMENT MEMBERS

Only Department members who have completed the required training and certification and are current on their certification will be allowed to access the CIBRS system. Certification will be verified by the agency administrator for the CIBRS system.

Department members who have met the certification requirements will be allowed to access the CIBRS database solely for the purposes listed below:

1. For the preparation of a case involving a criminal investigation being conducted by this agency.
2. To serve process in a criminal case.
3. To inform law enforcement of possible safety issues before service of process.
4. To enforce no contact orders.
5. To locate missing persons.
6. For the purpose of conducting a pre-employment background on a candidate for a *sworn* officer position.
7. To access the data at the request of the data subject.

ACCESS CIBRS BY THE DATA SUBJECT

Individuals requesting CIBRS data on themselves must specifically ask for data contained within the CIBRS system. The individual will be given a "CIBRS Request by Data Subject" form to complete. Upon completion of the form the subject will be required to produce a government issued photo ID. The name and date of birth on the government issued photo ID must exactly match the name and date of birth listed on the CIBRS Request by Data Subject form. The exact name and date of birth will be used to query CIBRS system. A report, which is automatically outputted to a printer, will be generated using the data subject information provided and the report will be given to the data subject. ***NOTE*** No record flagged as confidential within the CIBRS system shall be included in this report.

An individual may also request CIBRS data on themselves be forwarded to a third party. The subject will be given a "CIBRS Request by Data Subject for Informed Consent" form to complete. Upon completion of the form the subject will be required to produce a government issued photo ID. The name and date of birth on the government issued photo ID must exactly match the name and date of birth listed on the CIBRS Request by Data Subject Informed Consent Form. The exact name and date of birth will be used to query the CIBRS system. A report which is automatically outputted to a printer will be generated using the data subject information provided and given to the data subject who must then review and acknowledge the data contained within the report. To verify this, the data subject will be required to initial the CIBRS report. If after reviewing the report, the data subject still chooses to have the report forwarded to the third party, the Richfield Police Department will assume responsibility for mailing the report to the address provided on the CIBRS Request by Data Subject Informed Consent Form.

A parent or legal guardian may also request data from the CIBRS database on their juvenile child. The steps to ensure the identity of the requesting party listed above will be followed; additional some type of proof of parenthood should also be obtained (i.e. same address as parent on D.L. or ID, school issued ID, school record, court records, etc.)

CLASSIFICATION OF CIBRS DATA

No data contained within the CIBRS system is classified as public data, classification within the CIBRS system is as follows:

1. Confidential/Protected Non-Public: This applies to data which relates to an active case. This data is non-public and is not accessible to the subject of the data.
2. Private/Non-Public: This applies to data which relates to an inactive case or one which has not been updated in the CIBRS application for 120 days. This data is not accessible to the public, but is accessible to the data subject.

Only data which is Private/Non-Public will be released to the subject of the data or a third party at the request of the data subject. Data classified as Confidential/Protected Non-Public is related to an active case and will not be released to the subject of the data or a third party at their request. Requests for CIBRS data will be handled by the Chief of Police, CIBRS agency administrator, or the Support Services Supervisor.

CIBRS DATA NO LONGER NEEDED

Data which is no longer required for its intended purpose will be placed in a container to be shredded.

DATA VERIFICATION

Data obtained from the CIBRS database for the purpose of a criminal investigation and/or a pre-employment background check will be verified by contacting the responsible agency.

CIBRS DATA CHALLENGE

Upon the Richfield Police Department's participation in the CIBRS program as a submitting agency, (Richfield Police Department is the responsible agency) an individual may file a data challenge questioning the accuracy and/or completeness of the data. If a data challenge is received the following requirements must be met and actions taken:

1. The request must be made in writing by the subject of the data and their identity must be verified through a government issued photo ID. The request must describe the nature of the inaccuracies.
2. The challenge will be forwarded to the agency responsible authority (the Chief of Police or his/her designee). The responsible authority will then ensure that the record(s) in question is flagged within the CIBRS database as initiated.
3. Within 30 days the record challenged will be addressed and a determination will be made by the Chief of Police.
    a. Sustained challenges will be corrected or deleted upon determination. A letter will be sent to the data subject informing them of the results of their challenge to the data. The Richfield Police Department responsible authority will then update the CIBRS database marking the record in question as having sustained that challenge. CIBRS will then automatically notify the responsible authorities of all agencies that have viewed the record in question within the last year.
    b. If a challenge is not sustained and the data will not be altered, a letter will be sent to the data subject informing them of the results of their challenge. They will be informed that any appeal to this decision must be made to the Minnesota Department of Administration in Saint Paul. The responsible authority will then see that the flag that was previously placed on data is changed to declined.

If data change correction is received from another agency in regard to information this agency has obtained from the CIBRS database, the correction will be forwarded to the employee who originally obtained the data. The employee will then destroy the original data or replace with the updated data.

MISUSE OF THE CIBRS SYSTEM

Misuse of the CIBRS system is defined as:

1. Deliberate or intentional access for purposes not authorized by MSS 299C.40.
2. Repeated misuse whether intentional or unintentional
3. Intentional dissemination or failure to disseminate CIBRS data in accordance with the statute.

An employee of this department determined to have misused the CIBRS system will have their privilege to access the CIBRS system immediately revoked. The period of the revocation will be determined by the Chief of Police. The employee may also be subject to additional discipline per department policy (#104 General Standards of Conduct). The type of discipline and course of action will be determined by the Chief of Police.

Misuse of the CIBRS system may also carry sanctions for the employee or agency from the BCA. These sanctions will be honored and full cooperation will be given to the BCA audit staff. The BCA will conduct audits of the agency to ensure proper use of the CIBRS system. The Richfield Police Department will cooperate with the audit staff and provide the requested documents and verification.

By Order Of:

Chief of Police

CIBRS

Request by Data Subject

I, _____, am requesting a copy of the Request by
(Requestor name-please print)
Data Subject report from the Comprehensive Incident-Based Reporting System (CIBRS).

Requestor Information (as it appears on the government issued photo ID that will be presented to staff at the law enforcement agency as verification of identity – please print)

Last Name:_____

First Name:_____

Middle Name:_____

Date of Birth (Month/Day/Year):_____

Type of ID Presented: _____

_____ _____
Signature of Requestor Date

CIBRS Request by Data Subject
For Informed Consent

I, _____, am requesting a copy of the Request by
(Requestor name-please print)
Data Subject Report for Informed Consent from the Comprehensive Incident-Based Reporting System (CIBRS) as a part of an informed consent requirement from the below named party. After my review and acceptance of the data contained in the report, I am authorizing and requesting that the copy be sent to:

(Mailing Information for Company or specific individual requiring informed consent)

_____

_____

_____

for the purpose of

_____
(list reason for informed consent request – employment, housing, etc.)

Requestor Information (as it appears on the government issued photo ID that will be presented to staff at the law enforcement agency as verification of identity – please print)

Last Name: _____

First Name:_____

Middle Name: _____

Date of Birth (Month/Day/Year): _____

Type of ID Presented: _____

_____ _____
Signature of Requestor Date