Sioux Falls Police Department

Partnering with the community to serve, protect, and promote quality of life!

Policy: **Records Control**	Related Policies:	Section #: 1300 Records
		Policy #: 1301
		Effective: 6/2020
		Page 1 of 2
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can be used as basis of a complaint by this department for nonjudicial administrative action in accordance with the laws governing employee discipline.		
Policy Owner: ASD		
Reference: *South Dakota Records Retention Manual*		
Sensitivity Level: ☒ Public	☐ Law Enforcement Eyes Only	

1. Purpose:

    1.1. This policy is created to establish a policy regarding the control and security of law enforcement records and information.

2. Policy:

    2.1. Federal and state law closely regulates the collection and dissemination of criminal records information. Any criminal record information, or other confidential criminal justice information that may be contained in the department's records system, or within Sioux Falls Police Department, shall be confidential and may only be shared with other law enforcement agencies, officers, and/or other individuals in the criminal justice system.

3. Procedure:

    3.1. The integrity of reporting and maintenance of accurate, retrievable information is paramount. Official records will not be destroyed without authorization from the Police Chief in accordance with the state's retention policy.

    3.2. All records destruction will follow the guidelines outlined in the City of Sioux Falls Records and Retention Schedule.

    3.3. The Records Section shall maintain control of criminal records for use by all divisions and for planning of future operations.

3.4. Reports should be prepared, classified, indexed, and utilized in accordance with procedures specified by the Records Section.

3.5. Subpoenas, subpoenas duces tecum requests, or court orders for criminal record information will be processed by the Records Section Manager. The Sioux Falls Police Department Legal Advisor will be consulted for legal advice prior to the release of any criminal record information.

3.6. All police department personnel are responsible for the control of records information dissemination. No information available on the computer terminals will be given out to the general public, including vehicle registrations. Employees responsible for the improper release of information may be subject to criminal, civil, or departmental penalties.

3.7. All records requests shall be routed through the Records Section. This includes criminal requests, non-law enforcement related requests, or requests related to prospective employment.

3.7.1. Requests for criminal record information should be directed to the Records Manager, or in his/her absence, the Lead Records Clerk or the Administrative Captain.

3.8. All records requests shall be made in writing and must include the reason for the requested information. The Requests can be faxed to the Records section.

Sioux Falls Police Department

Partnering with the community to serve, protect, and promote quality of life!

Policy: **Forms and Reports**	Related Policies:	Section #: 1300 Records
		Policy #: 1302
		Effective: 6/2020
		Page 1 of 4
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can be used as basis of a complaint by this department for nonjudicial administrative action in accordance with the laws governing employee discipline.		
Policy Owner: ASD		
Reference:		
Sensitivity Level: ☒ Public	☐ Law Enforcement Eyes Only	

1. Purpose:

    1.1. This policy establishes policy regarding the proper use of forms and reports commonly used by the department.

2. Policy:

    2.1. Members of the Sioux Falls Police Department use a variety of different forms and reports during the course of their duties. These forms are to be complete and accurately reflect the circumstances that the author encounters. Law enforcement reports shall be completed during the same tour of duty in which the event necessitating the report occurred.

3. Procedure:

    3.1. Forms

        3.1.1. All department forms are maintained on file in the Records Section by the Records Section Manager.

        3.1.2. Any recommendations for new forms, changing existing forms, or discontinuance of existing forms must be presented to the Chief of Police through the chain of command for his approval.

3.1.3. Most investigative and administrative reports compiled by this department use a specific format. For this reason, the forms have been standardized for use by department personnel.

3.2. Reports

3.2.1. Report forms used by this department are either for operations or administrative purposes. Some require narrative form and others are of the completion or check-off type; i.e., mobile field reporting, to ensure inclusion of certain kinds of information.

3.2.2. Since all reports are intended to record information for future use by others, both inside and outside the department, as well as for the author's recollection, care must be exercised to ensure accuracy, clarity, and completeness.

3.2.3. Reports will be checked for accuracy and completeness by a supervisor during each shift. Incomplete, sloppy, or inaccurate reports will be returned for correction.

3.2.4. Reports shall be completed before officers complete their tour of duty.

3.2.5. All handwritten documents will be completed in black ink.

3.2.6. Several types of reports are recorded via telephone rather than completed by hand or computer.

3.2.6.1. Special care should be taken in preparing for the recording of these reports. The information should be complete and presented in a logical fashion. The narrator should speak clearly and distinctly and at a reasonably moderate speed. All proper names shall be complete and shall be spelled out for the Records Clerks. Any special punctuation or paragraphing should be related verbally to the Records Clerk while recording, especially when utilizing Speech Recognition Software.

3.2.6.2. Whenever an adult or juvenile is under custodial arrest, all recorded reports will be recorded priority. Priority recording will also be used in major cases and in cases requiring immediate follow-up.

3.2.6.3. Issues with report dictation are reported to the Records Section for resolution.

3.2.6.4. Officers are ultimately responsible for the review and accuracy of transcribed reports.

3.2.7. Administrative reports should be used to facilitate communications within the department and also with outside agencies.

3.2.8. Written communications with outside agencies shall be in the department name and identified by the author.

3.2.9. Operational reports are used to record all police action in performance of a service.

3.2.9.1. Telephonic Search Warrant (TSW)

3.2.9.1.1. The process of obtaining a warrant by means of telephonic affidavit for the search of a person to obtain blood or urine for the purpose of determining an accurate level of alcohol or drugs in their blood.

3.2.9.1.2. To be completed on a recorded line from within the Jail or the SFPD Report Room. Once the call is complete, officers will email the Records Manager to make notification of the warrant. Records will retrieve the audio and transcribe the details of the warrant verbatim. The completed TSW will be forwarded for review to the Sioux Falls Police Department Legal Advisor and back to the courts to be certified before eventually getting attached to the case.

3.3. Investigative Services Division Specific Forms

3.3.1. Case Status Form

3.3.1.1. To be completed and attached to all cases being sent to the State's Attorney's Office or City Attorney's Office for consideration of criminal charges. The Case Status Form will be routed back to the detective when a decision has been made and attached to the case.

3.3.2. Affidavit in Support of Arrest Warrant

3.3.2.1. A final summary and listing of probable cause to be sent along with the case copy and Case Status Form to the State's Attorney's Office or City Attorney's Office in application for an arrest warrant.

3.3.3. Consent to Search

3.3.3.1. Filled out by the investigating officer, signed and dated by the suspect. It authorizes a warrantless search of a premises or vehicle or other location for specified evidence of a specific crime.

3.3.4. Medical Release Authorization

3.3.4.1. A form authorizing a medical facility to release an individual's medical records pertaining to a specific injury/condition to police for use in a criminal investigation.

3.3.5. Affidavit in Support of Search Warrant

3.3.5.1. A standard format listing probable cause to support the issuance of a search warrant by a Magistrate or Circuit Court Judge for the search of a person, premise, or vehicle for specific evidence of a specified crime.

3.3.6. Search Warrant

3.3.6.1. Actual court order, directed to law enforcement, authorizing the search of a person, premise, or vehicle for specific evidence to aid in the investigation and prosecution of a specified crime.

3.3.7. Return of Search Warrant and Inventory.

3.3.7.1. A complete listing and inventory of items seized pursuant to a search warrant. The return must be signed by a Magistrate or Circuit Court Judge (preferably the Judge who authorized the warrant) and filed along with the Affidavit and Search Warrant in the Clerk of Court's Office.

3.3.8. Motion and Order to Release

3.3.8.1. A listing of all property that was seized pursuant to a search warrant and is no longer needed as evidence in any criminal prosecution or the subject of appeal. Must be prepared by the investigating officer and signed by a representative of the State's Attorney's Office and a Magistrate or Circuit Court Judge and filed in the Clerk of Court's Office prior to release of any property that was seized pursuant to a search warrant.

3.3.9. Evidence Inventory and Receipt

3.3.9.1. Multi-part receipt form to be completed by the investigating officer during the execution of a search warrant on a premises or vehicle that lists all items that were seized. The white original goes to the Police Records Section to be filed with the originals of the Case and Supplement Reports. The yellow copy is left at the scene of the search, or given to the subject of the search. The pink copy is sent to the Crime Lab/Evidence Section along with the items seized. In addition, a copy of the receipt will be made to be kept with the investigator's working file.

3.3.10. Stolen Property File

3.3.10.1. Blue “Add,” “Change,” “Delete” Form – Used to add, change, or delete descriptions of stolen property in the computerized file and NCIC. Filled out by the investigator and attached to the case when returned from Metro Communications and entries checked and verified.

Sioux Falls Police Department

Partnering with the community to serve, protect, and promote quality of life!

Policy: **CAD and Records Management System Downtime**	Related Policies:	Section #: 1300 Records
		Policy #: 1304
		Effective: 4/2023
		Page 1 of 2
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can be used as basis of a complaint by this department for nonjudicial administrative action in accordance with the laws governing employee discipline.		
Policy Owner: ASD		
Reference:		
Sensitivity Level: ☒ Public	☐ Law Enforcement Eyes Only	

1. Purpose:

1.1. The purpose of this policy is to provide department members with guidelines regarding the proper steps to follow during times of CAD and Records management System (RMS) disruption lasting for two hours or greater; or for downtime that occurs at or near the end of an officer's shift.

2. Policy:

2.1. It is the policy of the Sioux Falls Police Department to ensure that police incidents are accurately documented, and records management continues, even during times of network disruption. The reporting system is a necessary function of the criminal justice system of which we are a part and is essential to timely reporting to the courts and State's Attorney's Office.

3. Procedure:

3.1. Case Documentation

3.1.1. During CAD and RMS Disruptions as described above, officers will use the following report documents:

3.1.1.1. Sioux Falls Police Department Arrest Report (F210343)

3.1.1.2. Sioux Falls Police Department Case Report (F210001)

3.1.1.3. State of South Dakota Investigators Motor Vehicle Traffic Accident Report (DPS-AR1)

3.1.2. Printed copies of these forms can be found in the supply closet.

3.1.3. As officers document the facts of their arrest and case data, Marsy's Law details will need to be included accordingly.

3.1.4. Officers will turn in their documentation to Records before the end of their shift. Records Technicians will court prepare the documentation accordingly. If court preparation requirements are not a concern based on the time of day, Records will hold the paperwork until the RMS is functioning correctly.

3.1.5. Once the system is back in operation, Records will match the temporary case numbers with the updated case information provided by Metro Communications and will transfer the paper document details into the RMS.

3.2. Evidence Documentation

3.2.1. Officers will need to upload their evidence information to their OneDrive. Once the system is back in operation, officers are responsible for transferring the information on their drives to the corresponding case in the RMS.

3.3. Getac Documentation

3.3.1. Officers will classify their body camera and car videos with the temporary CFS provided by Metro Communications during downtimes. Once the system is back in operation, officers will cross reference the temporary number with the system assigned CFS.

Sioux Falls Police Department

Partnering with the community to serve, protect, and promote quality of life!

Policy: **Criminal Justice Information Media**	Related Policies:	Section #: 1300 Records
		Policy #: 1305
		Effective: 10/2024
		Page 1 of 4
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can be used as basis of a complaint by this department for nonjudicial administrative action in accordance with the laws governing employee discipline.		
Policy Owner: ASD		
Reference:		
Sensitivity Level: ☒ Public	☐ Law Enforcement Eyes Only	

1. Purpose:

   The intent of this policy is to ensure the protection of Criminal Justice Information (CJI) until information is either released to the public via authorized dissemination, i.e. within the court system or when presented in crime reports data, or until it's purged or destroyed in accordance with record retention guidelines. This applies to any authorized person who accesses stores, and/or transports electronic or physical media.

2. Policy:
   The intent of this policy is to ensure the protection of Criminal Justice Information (CJI) until information is either released to the public via authorized dissemination, i.e. within the court system or when presented in crime reports data, or until it's purged or destroyed in accordance with record retention guidelines. This applies to any authorized person who accesses stores, and/or transports electronic or physical media.

3. Procedure:
   3.1. Media Storage, Transport, and Access
   Sioux Falls Police Department personnel shall protect and maintain control of electronic and physical CJI at all times. The Sioux Falls Police Department will safeguard CJI to limit potential mishandling or loss while being stored, Sioux Falls Police Department personnel shall protect and maintain control of electronic and physical CJI at all times. The Sioux Falls Police Department will safeguard CJI to limit potential mishandling or loss while being stored, accessed, and/or

transported. Transporting CJI outside the agency's assigned physically secure areas must be monitored and controlled.
Any inadvertent or inappropriate CJI disclosure and/or use will be reported through the chain of command to the Sioux Falls Police Department Local Agency Security Officer (LASO) within one hour of the incident.
"Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.
To protect CJI, Sioux Falls Police Department personnel shall follow all established administrative, technical and physical safeguards to ensure the security and confidentiality of CJI including:accessed, and/or transported.
Transporting CJI outside the agency's assigned physically secure areas must be monitored and controlled.
Any inadvertent or inappropriate CJI disclosure and/or use will be reported through the chain of command to the Sioux Falls Police Department Local Agency Security Officer (LASO) within one hour of the incident.
"Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.
To protect CJI, Sioux Falls Police Department personnel shall follow all established administrative, technical and physical safeguards to ensure the security and confidentiality of CJI including:

3.1.1 Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.

3.1.2Restrict Access to electronic and physical media to authorized individuals.

3.1.3 Ensure that only authorized users remove printed forms or digital media from the CJI.

3.1.4 Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures.

3.1.5 Not use personally owned external flash drives or information systems to access, process, store, or transmit CJI unless specifically authorized by the Sioux Falls Police Department with established and documented specific terms and conditions.

3.1.6 Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

3.1.7 Store all hardcopy CJI printouts maintained by the Sioux Falls Police Department in a secure area accessible to only those employees whose job function requires them to handle such documents.

3.1.8 Take appropriate action when in possession of CJI while not in a secure area,

3.1.8.1 Take appropriate action when in possession of CJI while not in a secure area,

3.1.8.2 Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

3.1.8.2.1 When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

3.1.8.2.2 When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

3.2 Electronic Media Sanitization and Disposal

The Sioux Falls Police Department Crime Lab and City I.T. teams are responsible for properly sanitizing, that is, overwrite at least three times, or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable or court ordered disposed electronic media shall be destroyed (cut up, shredded, etc.). Physical media shall be securely disposed of when no longer required, using formal procedures. Documentation of the steps taken to sanitize or destroy electronic media is logged in the Central Square system or through written logs. When not done personally, City I.T. and Sioux

Falls Police personnel shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

3.3 Breach Notification and Incident Reporting

Employees shall promptly report breach of information or other information security incidents to their appropriate chain of command. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.
If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed.

3.3.1 Sioux Falls Police Department personnel shall notify his/her chain of command or LASO within one hour of the incident, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report will contain a detailed account of the incident, events leading to the incident, and steps taken or to be taken in response to the incident, which will be at the Sioux Falls Police Department's discretion.

3.3.2 Sioux Falls Police Department leadership will communicate any reported events to the LASO in order to make necessary notifications of the loss or disclosure of CJI records.

3.3.3 The LASO will ensure the CJIS System Agency Information Security Officer (CSA ISO) is promptly informed of security incidents.

3.3.4 Department leadership will notify City I.T. of incidents as needed, based on the situation or event. Incidents involving software applications will be handled by department leadership making notifications to the appropriate vendor personnel as needed, based on the situation.

3.3.5 If a cyber incident occurs, the following procedures must be immediately followed.

3.3.5.1 Sioux Falls Police Department will work with City I.T. and follow the appropriate city guidelines established to mitigate the incident properly.

3.3.5.2 The LASO will ensure the CJIS System Agency Information Security Officer (CSO/ISO) is promptly informed of the cyber incident.

3.3.5.3 Incidents involving software applications will be handled by department leadership notifying the appropriate vendor personnel.

3.3.5.4 The Sioux Falls Police Department LASO is the Records Manager.

3.4 Equipment Maintenance

The Sioux Falls Police Department participates in regular maintenance activities to preserve the life cycle of the equipment used throughout the department. Due to the variety of hardware and software used by the department, each item is handled uniquely, based on need, warranty factors, subscriptions, and service updates. For example, most of the hardware throughout the department is managed by the City I.T. team and maintenance work is documented through the internal ticketing system or Change Management Process. Most software programs used in the department are scheduled for maintenance and upgrade through the vendor and documented by them accordingly. For equipment requiring external maintenance (printers, scanning equipment, etc.), vendors must check in at the Police Front Desk and always be accompanied by authorized personnel. All employees are responsible for safeguarding CJI from unnecessary view or exposure while programs and equipment are being serviced.