Connect South Dakota Privacy, Civil Rights, and Civil Liberties Policy

A. Purpose Statement

1. The mission of the South Dakota Division of Criminal Investigation and each participating state and local law enforcement entity (PLEA) in joining the Joint Powers Agreement Establishing the Connect South Dakota Project (Joint Powers Agreement) is to facilitate the sharing of information, records and data in the possession of individual state and local law enforcement agencies (Originating PLEA), through the use of a state operated information sharing system (the Connect South Dakota System), for access and use by Acquiring PLEA in connection with ongoing law enforcement activities (Refer to Appendix B for definitions of Originating and Acquiring PLEAs). The purpose of this Privacy Policy is to promote conduct by the suppliers and users of the information acquired, stored, and shared through the Connect South Dakota System that complies with applicable federal, state, and local laws and assists the providers and users of this information in:

- Protecting individual privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of the criminal investigatory and other law enforcement retained information and records.
- Promoting governmental legitimacy and accountability.
- Not unduly burdening ongoing law enforcement activities.
- Making the most effective use of public resources allocated to law enforcement agencies.

B. Policy Applicability and Legal Compliance

1. All Connect South Dakota personnel, law enforcement and support personnel of PLEAs who are authorized to have access to or utilize the Connect South Dakota System, and private contractors providing information technology services associated with the Connect South Dakota Project will comply with the applicable provisions of this Privacy Policy. This Privacy Policy applies to information accessed, acquired, disclosed, or shared through the Connect South Dakota System.

2. Connect South Dakota, each PLEA, and private contractor(s) will provide a printed or electronic copy of this Privacy Policy to all authorized users of the Connect South Dakota System and to those who provide technology services for the Connect South Dakota Project and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

3. All Connect South Dakota and PLEA personnel utilizing the Connect South Dakota System, and private contractors providing technology services for the Connect South Dakota Project will comply with all applicable state, federal and local laws protecting confidentiality, privacy, civil rights and civil liberties, including, but not limited to laws listed in Appendix A of this Privacy Policy.

4. Connect South Dakota and each PLEA have adopted internal operating policies that are in compliance with applicable laws protecting confidentiality privacy, civil rights, and civil liberties (Refer to Appendix B).

C. Governance and Oversight

1. Primary responsibility for the day-to-day operation of the Connect South Dakota System, Connect South Dakota Project operations including the access to the system and the submission, dissemination, acquiring and sharing of information is assigned to the Connect South Dakota Administrator / DCI Assistant Director of Field Operations. Primary responsibility for enforcement of this Privacy Policy is assigned to the CSD Administrator / DCI Assistant Director of Field Operations (or designee) who is also appointed as the Connect South Dakota Privacy Officer.

2. The Connect South Dakota Project is guided by an oversight committee, including key PLEA stakeholder law enforcement agencies, whose activities include helping to ensure that confidentiality,

privacy and civil rights are protected as provided in this Privacy Policy and by Connect South Dakota Project information assimilation, dissemination and sharing processes and procedures. The committee will annually review and recommend updates to the policy in response to changes in law and implementation experience.

3. The oversight committee is guided by a trained Privacy Officer. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this Privacy Policy, receives and coordinates complaint resolution under the Connect South Dakota Project's redress policy, and serves as the liaison to help ensure that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: DCI Assistant Director of Field Operations, 1302 East Highway 14, Suite 5, Pierre, SD, 57501.

4. The Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N.3, Enforcement, of this Privacy Policy are adequate and enforced.

D. Definitions

1. Refer to Appendix B for definition of terms used in this Privacy Policy.

E. Information

1. To support PLEA law enforcement activities, the Connect South Dakota System is designed to facilitate the sharing of law enforcement information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law, or
- Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- Is useful in crime analysis or in the administration of criminal justice and public safety, and
- The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
- The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

2. The Connect South Dakota System will not seek or retain, and information-originating PLEAs will agree not to submit information to the Connect South Dakota System about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. The Connect South Dakota System may include "protected information," to include "personal data "on individuals or organizations that is entitled to protection under state and federal law or agency policy. Such information may be subject to confidentiality, privacy or other similar restrictions or limitations that affect access, use, or disclosure. The originating PLEA will label protected information (by record, data set or system of records) submitted to the Connect South Dakota System, to the maximum extent feasible pursuant to applicable limitations and restrictions on access and sensitivity of disclosure to:

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's or organization's right of privacy or civil rights and liberties.
- Provide legally required protections based upon an individual's status such as a juvenile or a victim.

4. Originating PLEA personnel will, to the extent feasible, upon receipt of information assess the information to determine or review its nature, usability, and quality. Originating PLEA will assign

categories to the information to reflect whether the information consists of incident, arrest, incarceration, booking, correctional, or other information category.

5. Originating PLEAs will enter and electronically associate certain basic descriptive metadata to information that will be submitted for sharing on the Connect South Dakota System for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information include:

- The name of the Originating PLEA, department of PLEA, or PLEA component and subcomponent.
- The name of the Originating PLEA information source (ex. booking, traffic arrest, accident investigation, etc.) from which the information is disseminated.
- The date the information was collected and, when feasible, the date its last accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information should be directed.

6. The Originating PLEA will attach, to the extent feasible, specific labels and descriptive metadata to information that will be used, accessed, or shared through the Connect South Dakota System to clearly indicate any legal restrictions on information sharing based on the information sensitivity or classification.

7. The labels and descriptive metadata assigned to existing information will be reevaluated by Originating PLEA entities whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

8. The PLEA originating the information shared through the Connect South Dakota System will keep a record of the source of all information submitted to the Connect South Dakota System.

F. Acquiring and Receiving Information

1. Information-gathering (acquisition) and access and investigative techniques used by Originating PLEAs, who submit information to the Connect South Dakota System, will remain in compliance with and will adhere to applicable laws, policies and guidance, including, but not limited to all applicable constitutional federal, state and local laws as well as applicable regulations and policies that apply to information databases. Refer to Appendix A for a listing of laws.

2. Information-gathering and investigative techniques used by the Originating PLEAs will be conducted in a reasonable, lawful, and authorized manner to gather information it is authorized to seek or retain.

3. Originating PLEAs will not directly or indirectly receive, seek, accept, retain or share information from:

- An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or Originating PLEA policy.
- An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

1. Originating PLEAs will make every reasonable effort to ensure that information submitted for sharing to the Connect South Dakota System is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information. The information submitted for sharing should, to the extent possible, contain all the fields required for information submission established by the Connect South Dakota Project. Additionally,

information will be merged with other information about the same individual or organization only when the applicable standard in Section I, Merging Records has been met.

2. At the time of retention in the Originating PLEA information system or at the time information is submitted to the Connect South Dakota System, the Originating PLEA will ensure information, to the maximum extent feasible, is complete and current.

3. The Originating PLEA will investigate, in a timely manner, alleged errors and deficiencies in information it submits for sharing to the Connect South Dakota System and corrects, deletes, or refrains from submitting information found to be erroneous or deficient.

4. The information retained in the Originating PLEA information system will be reevaluated by the Originating PLEA when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

5. The Originating PLEA will conduct proactive quality control reviews of information it originates and submits to the Connect South Dakota system and will make every reasonable effort to ensure that information that is found to be erroneous, misleading, obsolete, or otherwise unreliable will be corrected, deleted from the system, or not used.

6. Prior to taking action on information shared through Connect South Dakota, Acquiring PLEAs are responsible for reviewing the quality and verifying the accuracy of the information.

7. The Acquiring PLEA, upon review the quality and accuracy of information it has received from an Originating PLEA, will advise the appropriate contact person in the Originating PLEA, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

8. The Originating PLEA will use written or electronic notification to inform Acquiring PLEAs when information previously provided to the Acquiring PLEA is deleted or changed by the entity because the information is determined to be erroneous, or lacks adequate context such that the rights of the individual may be affected.

H. Collation and Analysis

1. Information obtained by the Acquiring PLEA through the Connect South Dakota System will be analyzed only by qualified individuals who have successfully completed a background check, if applicable, and have been selected, approved, and trained accordingly by the Acquiring PLEA.

2. Connect South Dakota System information subject to collation and analysis by an Acquiring PLEA is information as defined and identified in E. Information.

3. Information acquired or received by an Acquiring PLEA through the Connect South Dakota System is analyzed according to priorities and needs and will be analyzed only to further crime prevention, law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the entity.

I. Merging Records

1. Records entered in Connect South Dakota will not be merged with any other records. It is the responsibility of the Originating PLEA to make reasonable efforts to insure the accuracy of the data in the record prior to entering the record into the Connect South Dakota System.

J. Sharing and Dissemination

1. Credentialed, role-based access criteria established by the Connect South Dakota Project will be followed by all authorized users to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under what circumstances.

2. Access to or disclosure of records obtained by the Acquiring PLEAS or Private Contractors from the Connect South Dakota System will be provided only ***to persons within the entity or in other governmental entities*** who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, or as required to perform technology related services for the Connect South Dakota System or PLEA's information system, and only for the performance of official duties in accordance with law and procedures applicable to the entity for which the person is working.

3. Acquiring PLEAs may not disseminate information accessed, acquired or disseminated from an Originating PLEA, via the Connect South Dakota System, except as provided in the Joint Powers Agreement, without approval from the Originating PLEA. Acquiring PLEAs may allow information acquired from the Connect South Dakota System to be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law and in accordance with an existing Joint Powers Agreement, if applicable.

4. Access to or disclosure of information obtained by the Acquiring PLEAS from the Connect South Dakota System will be provided only ***to those responsible for public protection, public safety, or public health*** who are authorized to have access under law and the Joint Powers Agreement, and only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with law and procedures applicable to the entity for which the person is working.

5. Connect South Dakota System and the South Dakota Division of Criminal Investigation will maintain an audit trail of requested or disseminated information, including the date of the search and the search criteria. An audit trail will be kept for a minimum of two years.

6. Connect South Dakota will not disclose information ***to a member of the public***, except as provided in the procedure described in Section K. Redress, K.1 Disclosure.

7. Information submitted to the Connect South Dakota System or which was obtained from the Connect South Dakota System and retained by an Acquiring PLEA ***will not*** be:

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed or published without prior notice to the Originating PLEA that such information is subject to disclosure or publication, except to the extent provided per the provisions described in J. Sharing and Disclosure, Sections 2 - 4.
- Disseminated to persons not authorized to access or use the information.

8. Connect South Dakota personnel or Acquiring PLEAs shall not confirm the existence or nonexistence of information to any person or entity that would not be eligible to receive the information unless otherwise required by law.

K. Redress

K.1 Disclosure

1. Except as otherwise required by law, requests made to Connect South Dakota personnel or Acquiring PLEA from an individual or organization for disclosure, or a copy, of information about him or her, or the organization, will be in accordance with the provision described in J. Sharing and Disclosure, Section 8., such that Connect South Dakota personnel or Acquiring PLEAs shall not confirm the existence or nonexistence of information to any person or entity that would not be eligible to receive the information unless otherwise required by law. Individuals and organizations requesting information shall promptly be advised that such requests are to be made to the entity or organization that has care and custody of a record or document.

2. If Connect South Dakota personnel or Acquiring PLEA receives a request under the provisions of SDCL 1-27-35 to 43 for information or records located on the Connect South Dakota System or obtained by an Acquiring PLEA, Connect South Dakota personnel or the Acquiring PLEA shall respond in accordance with the provision described in J. Sharing and Disclosure, Section 8., and shall promptly advise the requestor that such requests are to be made to the entity or organization that has care and custody of a record or document.

Upon advising the requestor Connect South Dakota personnel and Acquiring PLEA will take no additional action regarding the request unless specifically requested by the entity or organization that has care and custody of the record or document, or so ordered by an authorized administrative or judicial officer with jurisdiction over the matter. A record will be kept of all requests for disclosure as provided in SDCL Chapter 1-27.

K.2 Corrections

1. If an individual or organization makes a request to Connect South Dakota personnel or an Acquiring PLEA for correction of information that has been disclosed by the entity or organization that has care and custody of a record or document, Connect South Dakota personnel or Acquiring PLEA shall respond in accordance with the provision described in J. Sharing and Disclosure, Section 8., and shall promptly advise the requestor that such requests for corrections are to be made to the entity or organization that has care and custody of a record or document. The Connect South Dakota personnel or Acquiring PLEA shall promptly notify the entity or organization that has care and custody of a record or document of the request for corrections. A record will be kept of all referrals of requests for corrections.

K.3 Appeals

1. For public records requests, appeal procedures are those provided in SDCL Chapter 1-27.

K.4 Complaints

1. If an individual has a complaint with regard to the accuracy or completeness of protected information that:

(a) Is exempt from disclosure.
(b) Has been or may be shared through the Connect South Dakota System.
    (1) Is held by the Connect South Dakota System, and
    (2) Allegedly has resulted in demonstrable harm to the complainant,

Connect South Dakota will refer the complaint to the entity or organization that has care and custody of a record or document who will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints may be submitted to the Connect South Dakota Privacy Officer at the following address: DCI Assistant Director of Field Operations, 1302 East Highway 14, Suite 5, Pierre, SD, 57501. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information in the Connect South Dakota System to the complainant unless otherwise required by law. The Connect South Dakota Privacy Officer will notify the Originating PLEA in writing or electronically within 14 days of receipt of the complaint and, upon request

by Connect South Dakota, the Originating PLEA will remove the record from the Connect South Dakota System and flag the record within the Originating PLEA's system such that it will not automatically load to Connect South Dakota. The Originating PLEA will then either purge the information so that it will not populate the Connect South Dakota system, or correct any identified data/record deficiencies or verify that the record is accurate prior to resubmitting the record to Connect South Dakota. All information submitted to Connect South Dakota that is the subject of a complaint will be reviewed by the Originating PLEA within 30 days. . If there is no resolution within 30 days, the Originating PLEA will not resubmit the record to the Connect South Dakota system until such time as the complaint has been resolved and the record corrected or confirmed to be accurate. A record will be kept by Connect South Dakota and the Originating PLEA of all complaints and the resulting action taken in response to the complaint.

L. Security Safeguards

1. The South Dakota Division of Criminal Investigation IT team leader is designated by the Director of the South Dakota Division of Criminal Investigation and trained to serve as the Connect South Dakota Project and Connect South Dakota Systems Security Officer.

2. The Connect South Dakota System will operate in a secure facility protected from external intrusion. The Connect South Dakota System will utilize secure internal and external safeguards against network intrusions. Connect South Dakota System information will only be accessible via secured access.

3. The Connect South Dakota System and Originating PLEAs will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

4. Access to information shared on the Connect South Dakota System will be granted only to PLEA personnel whose positions and job duties require such access; who have successfully completed a background check, if applicable; and who have been selected, approved, and trained accordingly.

5. Queries made to the Connect South Dakota System will be logged into the data system identifying the user initiating the query.

6. Connect South Dakota System and the South Dakota Division of Criminal Investigation will maintain an audit trail of requested or disseminated information, including the date of the search and the search criteria. An audit trail will be kept for a minimum of two years.

7. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

8. Upon discovery or notification of a data security breach of information shared through the Connect South Dakota System the Connect South Dakota Security Officer will notify the Originating PLEA and, if applicable, the Acquiring PLEA(s). Additionally, if an Acquiring PLEA or Originating PLEA discovers a data security breach of information shared through the Connect South Dakota System, the PLEA will notify the Connect South Dakota Security Officer. The Security Officer will coordinate with the PLEA to notify the individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

M. Information Retention and Destruction

1. Information retention and destruction of records submitted to Connect South Dakota by Originating PLEAs remains the responsibility of the Originating PLEA. As records are updated or purged in the Originating PLEA's system, they are updated or purged in the Connect South Dakota System through an automated process. All information shared through the Connect South Dakota System by Originating PLEA will be reviewed for record retention (validation or purge) by Originating PLEA in accordance with the Originating PLEA's records retention policy.

2. When information has no further value or meets the criteria for removal according to the Originating PLEA's records retention policy it will be purged, destroyed, and deleted or disposed of in accordance with the Originating PLEA's records retention policy.

3. An audit trail will be maintained by Connect South Dakota of information updated or purged from Connect South Dakota by Originating PLEA's automated process for a period of two years.

N. Accountability and Enforcement

N.1 Information System Transparency

1. Connect South Dakota is a statewide law enforcement information sharing service regarding information shared between Originating and Acquiring PLEAs, as such it does not gather or collect information. Information is shared through the Connect South Dakota System by Originating PLEAs for use by Acquiring PLEAs. PLEAs will be open with the public in regard to information collection practices. The Connect South Dakota Privacy Policy will be provided to the public for review, made available upon request, and posted on the Division of Criminal Investigations Web site at

http://dci.sd.gov/Services/ConnectSD.aspx

2. The Connect South Dakota Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the Connect South Dakota System. The Privacy Officer can be contacted at: DCI Assistant Director of Field Operations, 1302 East Highway 14, Suite 5, Pierre, SD, 57501.

N.2 Accountability

1. Queries made to the Connect South Dakota System will be logged into the data system identifying the name of the PLEA and the identity of the user initiating the query.

2. Connect South Dakota System and the South Dakota Division of Criminal Investigation will maintain an audit trail of requested or disseminated information, including the date of the search and the search criteria. An audit trail will be kept for a minimum of three years.

3. The Connect South Dakota Project will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this Privacy Policy. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least every three years, and a record of the audits will be maintained by the Privacy Officer. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the entity's information system(s). In addition, the South Dakota Division of Criminal Investigation will every three years conduct an audit and inspection of the information contained in the Connect South Dakota System.

4. Connect South Dakota personnel and PLEA personnel shall report suspected or confirmed violations of the Connect South Dakota Project policies relating to information shared on the Connect South Dakota System to the Connect South Dakota Privacy Officer.

5. The Connect South Dakota oversight committee, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this Privacy Policy annually and will recommend appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

N.3 Enforcement

1. If Connect South Dakota personnel, PLEA personnel, or Private Contractor personnel are found to be in noncompliance with the provisions of this Privacy Policy regarding information shared through the Connect South Dakota System, the Connect South Dakota Administrator will:

- Suspend or discontinue access to the Connect South Dakota System by the Connect South Dakota, PLEA, or Private Contractor personnel.
- Suspend, demote, transfer, or terminate Connect South Dakota personnel, as permitted by applicable personnel policies.
- If the authorized user is from a PLEA or Private Contractor, notify the PLEA or Private Contractor of identified noncompliance with the Privacy Policy and request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions. Personnel may be subject to administrative, civil, or criminal penalties as provided by applicable PLEA personnel policies, state and federal law.
- Contract with Private Contractor may be subject to termination or other authorized sanctions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The Connect South Dakota System reserves the right to restrict the qualifications and number of personnel having access to Connect South Dakota information and to suspend or withhold service and deny access to any PLEA or PLEA personnel violating this Privacy Policy.

O. Training

1. Each PLEA will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:

- All users authorized by PLEAs and information technology services personnel.
- Private contractors providing information technology services to the Connect South Dakota System or PLEA systems that house information passed through the Connect South Dakota System.

2. The Division of Criminal Investigation will require all personnel providing services to the Connect South Dakota Project to participate in training programs regarding the requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information, including information shared through the Information Sharing Environment.

3. The privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy.
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the entity.
- Originating and Acquiring PLEA responsibilities and obligations under applicable law and policy.
- How to implement the policy in the day-to-day work of the user.
- How to respond to non-law enforcement requests for Connect South Dakota information.

- The impact of improper activities associated with infractions of the Privacy Policy.
- Mechanisms for reporting violations of the Privacy Policy and Connect South Dakota Project procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A

OPEN RECORDS AND CONFIDENTIALITY STATUTES

STATE LAWS

SOUTH DAKOTA CODIFIED LAW
CHAPTER 1-27 PUBLIC RECORDS AND FILES

1-27-1 Public records open to inspection and copying.
1-27-1.1 Public records defined.
1-27-1.3 Liberal construction of public access to public records law--Certain criminal investigation and contract negotiation records exempt.
1-27-1.5 Certain records not open to inspection and copying.
1-27-1.6 Certain financial, commercial, and proprietary information exempt from disclosure.
1-27-1.7 Certain drafts, notes, and memoranda exempt from disclosure.
1-27-1.8 Certain records relevant to court actions exempt from disclosure.
1-27-1.9 Documents or communications used for decisional process arising from person's official duties not subject to compulsory disclosure.
1-27-1.10 Redaction of certain information.
1-27-1.13 Certain records not available to inmates.
1-27-1.14 Redaction of records in office of register of deeds not required.
1-27-1.15 Immunity for good faith denial or provision of record.
1-27-3 Records declared confidential or secret.
1-27-4 Format of open record.
1-27-9 Records management programs--Definition of terms.
1-27-15 Destruction of nonrecord materials.
1-27-16 Rules, standards, and procedures.
1-27-18 Local records management programs.
1-27-19 Annual meeting to authorize destruction of political subdivision records--Record of disposition.
1-27-21 "Public document or record" defined--Public meeting.
1-27-28 Definition of terms.
1-27-29 Disclosure of information concerning private entity restricted.
1-27-30 Confidentiality of proprietary or trade information of private entity.
1-27-31 Circumstances allowing for disclosure of information concerning private entity.
1-27-32 Disclosure of confidential information as misdemeanor.
1-27-33 Specific public access or confidentiality provisions not superseded by chapter provisions.
1-27-35 Informal requests for disclosure of records--Costs of retrieval or reproduction.
1-27-36 Estimate of retrieval and reproduction cost--Waiver or reduction of fee.
1-27-37 Written request for disclosure of records.
1-27-38 Civil action or administrative review of denial of written request or estimate of fees.
1-27-39 Response to notice of review.
1-27-40 Findings and decision of Office of Hearing Examiners.
1-27-40.1 Time for compliance with decision or appeal.
1-27-40.2 Costs, disbursements, and civil penalty for unreasonable, bad faith denial of access.
1-27-41 Appeal.

1-27-42 Public record officer for the state, county, municipality, township, school district, special district, or other entity.

1-27-1. Public records open to inspection and copying. Except as otherwise expressly provided by statute, all citizens of this state, and all other persons interested in the examination of the public records, as defined in § 1-27-1.1, are hereby fully empowered and authorized to examine such public record, and make memoranda and abstracts therefrom during the hours the respective offices are open for the ordinary transaction of business and, unless federal copyright law otherwise provides, obtain copies of public records in accordance with this chapter.

Each government entity or elected or appointed government official shall, during normal business hours, make available to the public for inspection and copying in the manner set forth in this chapter all public records held by that entity or official.

1-27-1.1. Public records defined. Unless any other statute, ordinance, or rule expressly provides that particular information or records may not be made public, public records include all records and documents, regardless of physical form, of or belonging to this state, any county, municipality, political subdivision, or tax-supported district in this state, or any agency, branch, department, board, bureau, commission, council, subunit, or committee of any of the foregoing. Data which is a public record in its original form remains a public record when maintained in any other form. For the purposes of §§ 1-27-1 to 1-27-1.15, inclusive, a tax-supported district includes any business improvement district created pursuant to chapter 9-55.

1-27-1.3. Liberal construction of public access to public records law--Certain criminal investigation and contract negotiation records exempt. The provisions of §§ 1-27-1 to 1-27-1.15, inclusive, and 1-27-4 shall be liberally construed whenever any state, county, or political subdivision fiscal records, audit, warrant, voucher, invoice, purchase order, requisition, payroll, check, receipt, or other record of receipt, cash, or expenditure involving public funds is involved in order that the citizens of this state shall have the full right to know of and have full access to information on the public finances of the government and the public bodies and entities created to serve them. Use of funds as needed for criminal investigatory/confidential informant purposes is not subject to this section, but any budgetary information summarizing total sums used for such purposes is public. Records which, if disclosed, would impair present or pending contract awards or collective bargaining negotiations are exempt from disclosure.

1-27-1.5. Certain records not open to inspection and copying. The following records are not subject to §§ 1-27-1, 1-27-1.1, and 1-27-1.3:

(1) Personal information in records regarding any student, prospective student, or former student of any educational institution if such records are maintained by and in the possession of a public entity, other than routine directory information specified and made public consistent with 20 U. S.C. 1232g, as such section existed on January 1, 2009;

(2) Medical records, including all records of drug or alcohol testing, treatment, or counseling, other than records of births and deaths. This law in no way abrogates or changes existing state and federal law pertaining to birth and death records;

(3) Trade secrets, the specific details of bona fide research, applied research, or scholarly or creative artistic projects being conducted at a school, postsecondary institution or laboratory funded in whole or in part by the state, and other proprietary or commercial information which if released would infringe intellectual property rights, give advantage to business competitors, or serve no material public purpose;

(4) Records which consist of attorney work product or which are subject to any privilege recognized in chapter 19-13;

(5) Records developed or received by law enforcement agencies and other public bodies charged with duties of investigation or examination of persons, institutions, or businesses, if the records constitute a part of the examination, investigation, intelligence information, citizen complaints or inquiries, informant identification, or strategic or tactical information used in law enforcement training. However, this subdivision does not apply to records so developed or received relating to the presence of and amount or concentration of alcohol or drugs in any body fluid of any person, and this subdivision does not apply to a 911 recording or a transcript of a 911 recording, if the agency or a court determines that the public interest in disclosure outweighs the interest in nondisclosure. This law in no way abrogates or changes §§ 23-5-7 and 23-5-11 or testimonial privileges applying to the use of information from confidential informants;

(6) Appraisals or appraisal information and negotiation records concerning the purchase or sale, by a public body, of any interest in real or personal property;

(7) Personnel information other than salaries and routine directory information;

(8) Information solely pertaining to protection of the security of public or private property and persons on or within public or private property, such as specific, unique vulnerability assessments or specific, unique response plans, either of which is intended to prevent or mitigate criminal acts, emergency management or response, or public safety, the public disclosure of which would create a substantial likelihood of endangering public safety or property; computer or communications network schema, passwords, and user identification names; guard schedules; lock combinations; or any blueprints, building plans, or infrastructure records regarding any building or facility that expose or create vulnerability through disclosure of the location, configuration, or security of critical systems;

(9) The security standards, procedures, policies, plans, specifications, diagrams, access lists, and other security-related records of the Gaming Commission and those persons or entities with which the commission has entered into contractual relationships. Nothing in this subdivision allows the commission to withhold from the public any information relating to amounts paid persons or entities with which the commission has entered into contractual relationships, amounts of prizes paid, the name of the prize winner, and the municipality, or county where the prize winner resides;

(10) Personally identified private citizen account payment information, credit information on others supplied in confidence, and customer lists;

(11) Records or portions of records kept by a publicly funded library which, when examined with or without other records, reveal the identity of any library patron using the library's materials or services;

(12) Correspondence, memoranda, calendars or logs of appointments, working papers, and records of telephone calls of public officials or employees;

(13) Records or portions of records kept by public bodies which would reveal the location, character, or ownership of any known archaeological, historical, or paleontological site in South Dakota if necessary to protect the site from a reasonably held fear of theft, vandalism, or trespass. This subdivision does not apply to the release of information for the purpose of scholarly research, examination by other public bodies for the protection of the resource or by recognized tribes, or the federal Native American Graves Protection and Repatriation Act;

(14) Records or portions of records kept by public bodies which maintain collections of archeological, historical, or paleontological significance which nongovernmental donors have requested to remain closed or which reveal the names and addresses of donors of such articles of archaeological, historical, or paleontological significance unless the donor approves disclosure, except as the records or portions thereof may be needed to carry out the purposes of the federal Native American Graves Protection and Repatriation Act and the Archeological Resources Protection Act;

(15) Employment applications and related materials, except for applications and related materials submitted by individuals hired into executive or policymaking positions of any public body;

(16) Social security numbers; credit card, charge card, or debit card numbers and expiration dates; passport numbers, driver license numbers; or other personally identifying numbers or codes; and financial account numbers supplied to state and local governments by citizens or held by state and local governments regarding employees or contractors;

(17) Any emergency or disaster response plans or protocols, safety or security audits or reviews, or lists of emergency or disaster response personnel or material; any location or listing of weapons or ammunition; nuclear, chemical, or biological agents; or other military or law enforcement equipment or personnel;

(18) Any test questions, scoring keys, results, or other examination data for any examination to obtain licensure, employment, promotion or reclassification, or academic credit;

(19) Personal correspondence, memoranda, notes, calendars or appointment logs, or other personal records or documents of any public official or employee;

(20) Any document declared closed or confidential by court order, contract, or stipulation of the parties to any civil or criminal action or proceeding;

(21) Any list of names or other personally identifying data of occupants of camping or lodging facilities from the Department of Game, Fish and Parks;

(22) Records which, if disclosed, would constitute an unreasonable release of personal information;

(23) Records which, if released, could endanger the life or safety of any person;

(24) Internal agency record or information received by agencies that are not required to be filed with such agencies, if the records do not constitute final statistical or factual tabulations, final instructions to staff that affect the public, or final agency policy or determinations, or any completed state or federal audit and if the information is not otherwise public under other state law, including chapter 15-15A and § 1-26-21;

(25) Records of individual children regarding commitment to the Department of Corrections pursuant to chapters 26-8B and 26-8C;

(26) Records regarding inmate disciplinary matters pursuant to § 1-15-20; and

(27) Any other record made closed or confidential by state or federal statute or rule or as necessary to participate in federal programs and benefits.

1-27-1.6. Certain financial, commercial, and proprietary information exempt from disclosure. The following financial, commercial, and proprietary information is specifically exempt from disclosure pursuant to §§ 1-27-1 to 1-27-1.15, inclusive:

(1) Valuable formulae, designs, drawings, computer source code or object code, and research data invented, discovered, authored, developed, or obtained by any agency if disclosure would produce private gain or public loss;

(2) Financial information supplied by or on behalf of a person, firm, or corporation for the purpose of qualifying to submit a bid or proposal;

(3) Financial and commercial information and records supplied by private persons pertaining to export services;

(4) Financial and commercial information and records supplied by businesses or individuals as part of an application for loans or program services or application for economic development loans or program services;

(5) Financial and commercial information, including related legal assistance and advice, supplied to or developed by the state investment council or the division of investment if the information relates to investment strategies or research, potential investments, or existing investments of public funds;

(6) Proprietary data, trade secrets, or other information that relates to:

(a) A vendor's unique methods of conducting business;

(b) Data unique to the product or services of the vendor; or

(c) Determining prices or rates to be charged for services, submitted by any vendor to any public body;

(7) Financial, commercial, and proprietary information supplied in conjunction with applications or proposals for funded scientific research, for participation in joint scientific research projects, for projects to commercialize scientific research results, or for use in conjunction with commercial or government testing;

(8) Any production records, mineral assessments, and trade secrets submitted by a permit holder, mine operator, or landowner to any public body.

1-27-1.7. Certain drafts, notes, and memoranda exempt from disclosure. Drafts, notes, recommendations, and memoranda in which opinions are expressed or policies formulated or recommended are exempt from disclosure pursuant to §§ 1-27-1 to 1-27-1.15, inclusive.

1-27-1.8. Certain records relevant to court actions exempt from disclosure. Any record that is relevant to a controversy to which a public body is a party but which record would not be available to another party under the rules of pretrial discovery for causes pending in circuit court are exempt from disclosure pursuant to §§ 1-27-1 to 1-27-1.15, inclusive.

1-27-1.9. Documents or communications used for decisional process arising from person's official duties not subject to compulsory disclosure. No elected or appointed official or employee of the state or any political subdivision may be compelled to provide documents, records, or communications used for the purpose of the decisional or deliberative process relating to any decision arising from that person's official duties.

1-27-1.10. Redaction of certain information. In response to any request pursuant to § 1-27-36 or 1-27-37, a public record officer may redact any portion of a document which contains information precluded from public disclosure by § 1-27-3 or which would unreasonably invade personal privacy, threaten public safety and security, disclose proprietary information, or disrupt normal government operations. A redaction under this section is considered a partial denial for the application of § 1-27-37.

1-27-1.13. Certain records not available to inmates. The secretary of corrections may prohibit the release of information to inmates or their agents regarding correctional operations, department policies and procedures, and inmate records of the requesting inmate or other inmates if the release would jeopardize the safety or security of a person, the operation of a correctional facility, or the safety of the public. This section does not apply to an inmate's attorney requesting information that is subject to disclosure under this chapter.

1-27-1.15. Immunity for good faith denial or provision of record. No civil or criminal liability may attach to a public official for the mistaken denial or provision of a record pursuant to this chapter if that action is taken in good faith.

1-27-3. Records declared confidential or secret. Section 1-27-1 shall not apply to such records as are specifically enjoined to be held confidential or secret by the laws requiring them to be so kept.

1-27-4. Format of open record. Any record made open to the public pursuant to this chapter shall be maintained in its original format or in any searchable and reproducible electronic or other format. This chapter does not mandate that any record or document be kept in a particular format nor does it require that a record be provided to the public in any format or media other than that in which it is stored.

1-27-9. Records management programs--Definition of terms. Terms used in §§ 1-27-9 to 1-27-18, inclusive, mean:

(1) "Local record," a record of a county, municipality, township, district, authority, or any public corporation or political entity whether organized and existing under charter or under general law, unless the record is designated or treated as a state record under state law;

(2) "Record," a document, book, paper, photograph, sound recording, or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included within the definition of records as used in §§ 1-27-9 to 1-27-18, inclusive;

(3) "State agency" or "agency" or "agencies," includes all state officers, boards, commissions, departments, institutions, and agencies of state government;

(4) "State record," :

(a) A record of a department, office, commission, board, or other agency, however designated, of the state government;

(b) A record of the State Legislature;

(c) A record of any court of record, whether of state-wide or local jurisdiction;

(d) Any other record designated or treated as a state record under state law.

1-27-15. Destruction of nonrecord materials. Any nonrecord material not included within the definition of records as contained in § 1-27-9 may be destroyed at any time by the agency in possession of such materials without the prior approval of the commissioner of administration.

1-27-18. Local records management programs. The governing body of each county, municipality, township, district, authority, or any public corporation or political entity, whether organized and existing under charter or under general law, shall promote and implement the principles of efficient records management for local records. The governing body may, as far as practical, follow the program established for the management of state records. The commissioner of administration may, upon the request of a governing body, provide advice and assistance in the establishment of a local records management program.

1-27-19. Annual meeting to authorize destruction of political subdivision records--Record of disposition. The State Record Destruction Board shall meet at least once each year and consider requests of all political subdivisions for the destruction of records and to authorize their destruction as in the case of state records. However, in the case of any records recommended to be destroyed, the board shall require a record to be kept of the disposition of the documents.

1-27-21. "Public document or record" defined--Public meeting. For the purposes of §§ 1-27-20 to 1-27-26, inclusive, an official public document or record is any document officially compiled, published, or recorded by the state including deeds, publicly probated wills, records of births, deaths, and marriages, and any other document or record required to be kept open for public inspection pursuant to chapter 1-27. An official public meeting is any meeting or proceeding required to be open to the public pursuant to chapter 1-25.

1-27-28. Definition of terms. Terms used in §§ 1-27-29 to 1-27-32, inclusive, mean:

(1) "Private entity," any person or entity that is not a public entity as defined by subdivision 3-21-1(2);

(2) "State agency," any association, authority, board, commission, committee, council, department, division, office, officer, task force, or other agent of the state vested with the authority to exercise any portion of the state's sovereignty. The term does not include the Legislature, the Unified Judicial System, the Public Utilities Commission, the Department of Environment and Natural Resources, any law enforcement agency, or any unit of local government, or joint venture comprised of local governments;

(3) "Financial investigation, examination, or audit," any examination conducted by a state agency of a private entity's proprietary information or trade secret information;

(4) "Proprietary information," information on pricing, costs, revenue, taxes, market share, customers, and personnel held by private entities and used for that private entity's business purposes;

(5) "Trade secret," information, including a formula, pattern, compilation, program, device, method, technique, process, marketing plan, or strategic planning information that:

(a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

1-27-29. Disclosure of information concerning private entity restricted. No state agency may disclose that it is conducting a financial investigation, examination, or audit of a private entity while the financial investigation, examination, or audit is ongoing, except as provided by § 1-27-31.

1-27-30. Confidentiality of proprietary or trade information of private entity. All proprietary or trade secret information obtained by a state agency from or concerning a private entity is confidential, except as provided by § 1-27-31.

1-27-31. Circumstances allowing for disclosure of information concerning private entity. A state agency may disclose that it is conducting a financial investigation, examination, or audit of a private entity and disclose the information obtained from such an investigation, examination, or audit as follows:

(1) To the private entity being investigated, examined, or audited;

(2) To those persons whom the private entity has authorized in writing to receive such information;

(3) To the officers, employees, or legal representatives of any other state agency which requests the information in writing for the purpose of investigating and enforcing civil or criminal matters. The written request will specify the particular information desired and the purpose for which the information is requested;

(4) To any administrative or judicial body if the information is directly related to the resolution of an issue in the proceeding, or pursuant to an administrative or judicial order. However, no person may use a subpoena, discovery, or other applicable statutes to obtain such information;

(5) To another state pursuant to an agreement between the State of South Dakota and the other state, but only if the other state agrees to keep the information confidential as set forth in §§ 1-27-28 to 1-27-32, inclusive;

(6) To the attorney general, state's attorney, or any state, federal, or local law enforcement officer;

(7) To a federal agency pursuant to the provisions of federal law;

(8) To the extent necessary to submit any final reports or filings which are otherwise required by law to be prepared or filed;

(9) Repealed by SL 2004, ch 25, § 4.

(10) To comply with federal law, rules, or program delegation requirements ; or

(11) To the extent necessary to protect the health or welfare of the citizens of this state or nation pursuant to a court order obtained under the same process as orders issued pursuant to § 15-6-65(b).

1-27-32. Disclosure of confidential information as misdemeanor. Disclosure of information made confidential by §§ 1-27-28 to 1-27-32, inclusive, except as provided in § 1-27-31, is a Class 1 misdemeanor.

1-27-33. Specific public access or confidentiality provisions not superseded by chapter provisions. The provisions of this chapter do not supersede more specific provisions regarding public access or confidentiality elsewhere in state or federal law.

1-27-35. Informal requests for disclosure of records--Costs of retrieval or reproduction. Any informal request for disclosure of documents or records shall be made to the custodian of the record. The custodian of the record may then provide the requestor with the document or record upon payment of the actual cost of mailing or transmittal, the actual cost of reproduction, or other fee established by statute or administrative rule. A requestor that makes an informal request requiring the dedication of staff time in excess of one hour may be required to pay the cost of the staff time necessary for the location, assembly, or reproduction of the public record. If any records are required or permitted to be made public upon request and no other rate is prescribed for reproduction or retrieval of such records, the Bureau of Administration shall establish, by rules promulgated pursuant to chapter 1-26, the maximum rate, or the formula for calculating rates, for reproduction and retrieval.

1-27-36. Estimate of retrieval and reproduction cost--Waiver or reduction of fee. For any informal request reasonably likely to involve a fee in excess of fifty dollars, the custodian shall provide an estimate of cost to the requestor prior to assembling the documents or records and the requestor shall confirm in writing his or her acceptance of the cost estimate and agreement to pay. The custodian may exercise discretion to waive or reduce any fee required under this section if the waiver or reduction of the fee would be in the public interest.

1-27-37. Written request for disclosure of records. If an informal request is denied in whole or in part by the custodian of a document or record, a written request may be made by the requestor pursuant to this section:

(1) A written request may be made to the public record officer of the public entity involved. The public record officer shall promptly respond to the written request but in no event later than ten business days from receipt of the request. The public record officer shall respond to the request by:

(a) Providing the record in whole or in part to the requestor upon payment of any applicable fees pursuant to §§ 1-27-35 and 1-27-36;

(b) Denying the request for the record; or

(c) Acknowledging that the public record officer has received the request and providing an estimate of the time reasonably required to further respond thereto;

(2) Additional time to respond to the written request under subsection (1)(c) of this section may be based upon the need to clarify the nature and scope of the written request, to locate and assemble the information requested, to notify any third persons or government agencies affected by the written request, or to determine whether any of the information requested is not subject to disclosure and whether a denial should be made as to all or part of the written request;

(3) If a written request is unclear, the public record officer may require the requestor to clarify which records are being sought. If the requestor fails to provide a written response to the public record officer's request for clarification within ten business days, the request shall be deemed withdrawn and no further action by the public records officer is required;

(4) If the public record officer denies a written request in whole or in part, the denial shall be accompanied by a written statement of the reasons for the denial;

(5) If the public record officer fails to respond to a written request within ten business days, or fails to comply with the estimate provided under subsection (1)(3) of this section without provision of a revised estimate, the request shall be deemed denied.

1-27-38. Civil action or administrative review of denial of written request or estimate of fees. If a public record officer denies a written request in whole or in part, or if the requestor objects to the public record officer's estimate of fees or time to respond to the request, a requestor may within ninety days of the denial commence a civil action by summons or, in the alternative, file a written notice of review with the Office of Hearing Examiners. The notice of review shall be mailed, via registered or certified mail, to the

Office of Hearing Examiners and shall contain:

(1) The name, address, and telephone number of the requestor;

(2) The name and business address of the public record officer denying the request;

(3) The name and business address of the agency, political subdivision, municipal corporation, or other entity from which the request has been denied;

(4) A copy of the written request;

(5) A copy of any denial or response from the public record officer; and

(6) Any other information relevant to the request that the requestor desires to be considered.

1-27-39. Response to notice of review. Upon receipt, the Office of Hearing Examiners shall promptly mail a copy of the notice of review filed pursuant to § 1-27-38 and all information submitted by the requestor to the public record officer named in the notice of review. The entity denying the written request may then file a written response to the Office of Hearing Examiners within ten business days. If the entity does not file a written response within ten business days, the Office of Hearing Examiners shall act on the information provided. The Office of Hearing Examiners shall provide a reasonable extension of time to file a written response upon written request or agreement of parties.

1-27-40. Findings and decision of Office of Hearing Examiners. Upon receipt and review of the submissions of the parties, the Office of Hearing Examiners shall make written findings of fact and conclusions of law, and a decision as to the issue presented. Before issuing a decision, the Office of Hearing Examiners may hold a hearing pursuant to chapter 1-26 if good cause is shown.

1-27-40.1. Time for compliance with decision or appeal. If the office of hearing examiners enters a decision pursuant to § 1-27-40 concluding that certain records shall be released or that the fee charged pursuant to §§ 1-27-35 and 1-27-36 was excessive, the public entity has thirty days after the opinion is issued to comply with the order or to file an appeal pursuant to § 1-27-41.

1-27-40.2. Costs, disbursements, and civil penalty for unreasonable, bad faith denial of access. In a civil action filed pursuant to § 1-27-38 or upon an appeal filed pursuant to § 1-27-41, if the court determines that the public entity acted unreasonably and in bad faith the court may award costs, disbursements, and a civil penalty not to exceed fifty dollars for each day that the record or records were delayed through the fault of the public entity. Any civil penalty collected pursuant to this section shall be deposited into the state general fund.

1-27-41. Appeal. The aggrieved party may appeal the decision of the Office of Hearing Examiners to the circuit court pursuant to chapter 1-26. In any action or proceeding under §§ 1-27-35 to 1-27-43, inclusive, no document or record may be publicly released until a final decision or judgment is entered ordering its release.

1-27-42. Public record officer for the state, county, municipality, township, school district, special district, or other entity. The public record officer for the state is the

secretary, constitutional officer, elected official, or commissioner of the department, office, or other division to which a request is directed. The public record officer for a county is the county auditor or the custodian of the record for law enforcement records. The public record officer for a first or second class municipality is the finance officer or the clerk or the custodian of the record for law enforcement records. The public record officer for a third class municipality is the president of the board of trustees or the custodian of the record for law enforcement records. The public record officer for an organized township is the township clerk. The public record officer for a school district is the district superintendent or CEO. The public record officer for a special district is the chairperson of the board of directors. The public record officer for any other entity not otherwise designated is the person who acts in the capacity of the chief financial officer or individual as designated by the entity.

CHAPTER 10-1 DEPARTMENT OF REVENUE

10-1-25. Investigation of evasions and violations of tax and assessment laws--Proceedings to remedy improper administration. The secretary of revenue shall examine all cases in which evasions or violations of the laws of this state relating to the assessment and taxation of property are complained of or discovered. The secretary shall examine all cases in which property subject to taxation has not been assessed or has been fraudulently or for any reason improperly or unequally assessed or in which the laws in any manner have been evaded or violated. The secretary shall institute proceedings to remedy improper or negligent administration of the laws relating to the taxing of property in the state.

10-1-26. Summons of witnesses and evidence in departmental investigations. The secretary of revenue may summon witnesses to appear and give testimony and to produce records, books, papers, and documents relating to any matter on which the secretary has authority to investigate or determine.

10-1-27. Depositions in departmental investigations. The secretary of revenue shall cause the deposition of witnesses residing within or without the state or absent from the state to be taken upon notice to the interested person, if any, in like manner that depositions of witnesses are taken in civil actions pending in the circuit court, in any matter on which the secretary has authority to investigate or determine.

10-1-28. Administration of oaths to witnesses--Proceedings on refusal of witness to testify or produce evidence--Compensation of witnesses and officers serving summons--False testimony as perjury. The secretary of revenue, in any matter under investigation or consideration, may administer oaths to witnesses. If any witness fails to obey any summons to appear before the secretary, refuses to testify or answer any question, or fails to produce records, books, papers, or documents if required so to do, such failure or refusal shall be reported to the attorney general who shall institute proceedings in the proper circuit court to compel obedience to any summons or order of the secretary. Officers who serve summonses or subpoenas and witnesses attending shall receive like compensation as officers and witnesses in the circuit court. Such compensation shall be paid by the county for whose benefit the investigation is made, upon certificate of the secretary of revenue.

Any person who testifies falsely in any matter under consideration by the secretary of revenue in an investigation as provided in this section is guilty of perjury.

10-1-28.1. Confidentiality of return information--Definition of terms. Terms used in §§ 10-1-28.1 to 10-1-28.5, inclusive, mean:

(1) "Department," the Department of Revenue;

(2) "Return information," any information collected, prepared or received by the department which relates to a return, including the nature or amount of a taxpayer's income, receipts, deductions, net worth, tax liability, or deficiencies, or any part of any written determination or background file documents relating to such information. The term does not include data in a form which cannot be associated with or otherwise identify, directly or indirectly, a particular taxpayer;

(3) "Returns," all tax returns, tax reports or claims for refund which are filed with the Department of Revenue, except those returns or claims for refund filed under the provisions of chapters 10-28 to 10-38, inclusive;

(4) "Secretary," the secretary of the Department of Revenue.

10-1-28.2. Lists compiled by department confidential--Unauthorized disclosure as misdemeanor. All lists of taxpayers, licensees, or applicants compiled by the Department of Revenue are confidential except licensees which were licensed under the provisions of chapter 10-47B, 32-6B, 32-6C, or 32-7A. It is a Class 2 misdemeanor to disclose any such list except to the extent necessary to carry out the official duties of the department.

10-1-28.3. Return information confidential--Unauthorized disclosure as misdemeanor. Returns and return information are confidential. It is a Class 1 misdemeanor to disclose such information except in accordance with §§ 10-1-28.4 and 10-1-28.5.

10-1-28.4. Persons to whom return information may be disclosed--Purposes. Returns and return information may be disclosed to the following:

(1) The taxpayer who is required to submit the information to the department, or his designee appointed in writing;

(2) Other states, in accordance with agreements executed pursuant to § 10-1-13.1;

(3) Any agency, body, commission, or legal representative of the United States charged with the administration of the United States tax laws for the purpose of, and only to the extent necessary in, the administration of such laws;

(4) Officers, employees or legal representatives of the Department of Revenue, but only to the extent necessary to carry out their official duties;

(5) Officers, employees or legal representatives of any other state agency or department or political subdivision of the state for a civil or criminal law enforcement activity, if the head of the agency, department or political subdivision desiring such information has made a written request to the secretary specifying the particular information desired and the law enforcement activity for which the information is sought;

(6) Officers, employees or legal representatives of the commission on gaming and the lottery commission for the purpose of, and only to the extent necessary for, the administration of chapters 42-7A and 42-7B.

10-1-28.5. Disclosure of return information in judicial or administrative proceedings. Returns and return information may be disclosed in a judicial or administrative proceeding:

(1) If the information is directly related to the resolution of an issue in the proceeding; or

(2) To the extent required by a proper judicial or administrative order.

10-1-28.6. Federal taxpayer information defined. Federal taxpayer information means a federal tax return or portion thereof, or information reflected thereon, which the state requires a taxpayer to attach to, or include in, any state tax return. The term does not include data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer.

10-1-28.7. Federal taxpayer information confidential--Unauthorized disclosure as misdemeanor. All federal taxpayer information is confidential. It is a Class 1 misdemeanor to disclose such information except in accordance with § 10-1-28.8 or 10-1-28.9.

10-1-28.8. Persons to whom federal taxpayer information may be disclosed--Purposes. Federal taxpayer information may be disclosed to:

(1) The taxpayer who is required to submit the information to the state, or his designee appointed in writing;

(2) Officers, employees, or legal representatives of the state agency or department receiving or collecting the information, but only to the extent necessary to carry

out their official duties; and

(3) Officers, employees, or legal representatives of any state agency or department for a civil or criminal law enforcement activity if the head of the agency or department has made a written request to the department having the information in which is specified the particular information desired and the law enforcement activity for which the information is sought.

10-1-28.9. Disclosure of federal taxpayer information in judicial or administrative proceedings. Returns and return information may be disclosed in a judicial or administrative proceeding:

(1) If the information is directly related to the resolution of an issue in the proceeding; or

(2) To the extent required by a proper judicial or administrative order..

CHAPTER 15-15A UNIFIED JUDICIAL SYSTEM COURT RECORDS RULE

15-15A-3. Definition of terms. (1) "Court record" includes any document, information, or other thing that is collected, received or maintained by a clerk of court in connection with a judicial proceeding. "Court record" does not include other records maintained by the public official who also serves as clerk of court or information gathered, maintained or stored by a governmental agency or other entity to which the court has access but which is not part of the court record as defined in this section.

(2) Information in a court record "in electronic form" includes information that exists as: (a) electronic representations of text or graphic documents; (b) an electronic image, including a video image, of a document, exhibit or other thing; or (c) data in the fields or files of an electronic database.

(3) "Public access" means that the public may inspect and obtain a copy of the information in a court record unless otherwise prohibited by statute, court rule or a decision by a court of competent jurisdiction. The public may have access to inspect information in a court file upon payment of applicable fees.

(4) "Remote access" means the ability to electronically search, inspect, or copy information in a court record without the need to physically visit the court facility where the court record is maintained.

15-15A-4. Applicability of rule. This rule applies to all court records, regardless of the physical form of the court record, the method of recording the information in the court record or the method of storage of the information in the court record.

15-15A-5. General access rule. (1) Information in the court record is accessible to the public except and as prohibited by statute or rule and except as restricted by §§ 15-15A-7 through 15-15A-13.

(2) There shall be a publicly accessible indication of the existence of information in a court record to which access has been restricted, which indication shall not disclose the nature of the information protected, i.e., "sealed document."

(3) An individual circuit or a local court may not adopt a more restrictive access policy or otherwise restrict access beyond that provided by statute or in this rule, nor provide greater access than that provided for by statute or in this rule.

15-15A-7. Court records excluded from public access. The following information in a court record is not accessible to the public:

(1) Information that is not to be accessible to the public pursuant to federal law;

(2) Information that is not to be accessible to the public pursuant to state law, court rule or case law as follows;

(3) Examples of such state laws, court rules, or case law follow. Note this may not be a complete listing and the public and court staff are directed to consult state law, court rules or case law. Note also that additional documents are listed below that may not be within court records but are related to the court system; the public and court staff should be aware of access rules relating to these documents.

(a) Abortion records (closed); § 34-23A-7.1

(b) Abuse and neglect files and records (closed, with statutory exceptions); § 26-8A-13

(c) Adoption files and adoption court records (closed, with statutory exceptions); §§ 25-6-15 through 25-6-15.3

(d) Affidavit filed in support of search warrant (sealed if so ordered by court, see statutory directives); § 23A-35-4.1

(e) Attorney discipline records (closed until formal complaint has been filed with Supreme Court by the State Bar Association's Disciplinary Board or Attorney General, accused attorney requests matter be public, or investigation is premised on accused attorney's conviction of a crime); § 16-19-99

(f) Civil case filing statements (closed); § 15-6-5(h);

(g) Coroner's inquest (closed until after arrest directed if inquisition finds criminal involvement with death); § 23-14-12

(h) Custody or visitation dispute mediation proceedings pursuant to § 25-4-60 (closed, inadmissible into evidence)

(i) Discovery material (closed unless admitted into evidence by court) §§ 15-6-26(c); 15-6-5(g)

(j) Domestic abuse victim's location (closed, with statutory exception); § 25-10-39

(k) Employment examination or performance appraisal records maintained by Bureau of Personnel (closed); § 1-27-1

(l) Grand jury proceedings (closed with statutory exceptions); § 23A-5-16

(m) Guardianships and conservatorships (closed with statutory exceptions); § 29A-5-311

(n) Involuntary commitment for alcohol and drug abuse (petition, application, report to circuit court and court's protective custody order sealed; law enforcement or prosecutor may petition the court to examine these documents for limited purpose); § 34-20A-70.2

(o) Judicial disciplinary proceedings (closed until Judicial Qualifications Commission files its recommendation to Supreme Court, accused judge requests matter be public, or investigation is premised on accused judge's conviction of either a felony crime or one involving moral turpitude); ch. 16-1A, Appx. III(1)

(p) Juvenile court records and court proceedings (closed with statutory exception); §§ 26-7A-36 through -38; §§ 26-7A-113 through -116

(q) Mental illness court proceedings and court records (closed); §§ 27A-12-25; 27A-12-25.1 through -32

(r) Pardons (statutory exceptions, see § 24-14-11)

(s) Presentence investigation reports (closed); §§ 23A-27-5 through -10; § 23A-27-47

(t) Probationer under suspended imposition of sentence (record sealed upon successful completion of probation conditions and discharge); §§ 23A-27-13.1; 23A-27-17

(u) Records prepared or maintained by court services officer (closed except by specific order of court); § 23A-27-47

(v) Trade secrets (closed); subdivision 15-6-26(c)(7)

(w) Trusts (sealed upon petition with statutory exceptions); § 21-22-28

(x) Voluntary termination of parental rights proceedings and records (closed except by order of court); § 25-5A-20

(y) Wills (closed with statutory exceptions); § 29A-2-515

(z) Written communication between attorney and client; attorney work product (closed unless such privilege is waived); ch. 16-18, Appx. Rule 1.6

(aa) Information filed with the court pending in camera review (closed)

(bb) Any other record declared to be confidential by law; § 1-27-3.

15-15A-8. Confidential numbers and financial documents excluded from public access. The following information in a court record is not accessible to the public.

(1) Social security numbers, employer or taxpayer identification numbers, and financial account numbers of a party or party's child.

(2) Financial documents such as income tax returns, W-2's and schedules, wage stubs, credit card statements, financial institution statements, credit card account statements, check registers, and other financial information.

15-15A-9. Filing confidential number and financial documents in the court record. (1) Social security numbers, employer or taxpayer identification numbers, and financial account numbers of a party or party's child, where required to be filed with the court shall be submitted on a separate Confidential Information Form, appended to these rules, and filed with the pleading or other document required to be filed. The Confidential Information Form is not accessible to the public.

(2) Financial documents named in subdivision 15-15A-8(2) that are required to be filed with the court shall be submitted as a confidential document and designated as such to the clerk upon filing. The Confidential Financial Documents Information Form appended to these rules shall be attached to financial documents being filed with the court. The Confidential Financial Documents Information Form is not accessible to the public. The confidential financial documents will not be publicly accessible, even if admitted as a trial or hearing exhibit, unless the court permits access pursuant to § 15-15A-10. The court may, on its own motion, protect financial documents that have been submitted without the Confidential Financial Documents Information Form.

(3) Parties with cases filed prior to the effective date of this rule, or the court on its own, may, by motion, protect the privacy of confidential information as defined in § 15-15A-8. Parties filing this motion will submit a completed Confidential Information Form or Confidential Financial Documents Information Form as appropriate.

CHAPTER 19-13 PRIVILEGES

19-13-22 (Rule 509(a)) Governmental investigative agency's privilege as to identity of informer.
19-13-23 (Rule 509(b)) Persons entitled to claim governmental investigative privilege.
19-13-24 (Rule 509(c)(1)) Informer privilege not applicable if identity otherwise disclosed.
19-13-25 (Rule 509(c)(2)) In camera proceedings to determine whether informer should be identified--Relief to opposing party--Protective measures.
19-13-33 Privileged communications concerning execution of inmate.

19-13-22. (Rule 509(a)) Governmental investigative agency's privilege as to identity of informer. The United States or a state or subdivision thereof has a privilege to refuse to disclose the identity of a person who has furnished information relating to or assisting in an investigation of a possible violation of a law to a law enforcement officer or member of a legislative committee or its staff conducting an investigation.

19-13-23. (Rule 509(b)) Persons entitled to claim governmental investigative privilege. The privilege described by § 19-13-22 may be claimed by an appropriate representative of the public entity to which the information was furnished.

19-13-24. (Rule 509(c)(1)) Informer privilege not applicable if identity otherwise disclosed. No privilege exists under § 19-13-22 if the identity of the informer or his interest in the subject matter of his communication has been disclosed to those who would have cause to resent the communication by a holder of the privilege or by the informer's own action, or if the informer appears as a witness for the government.

19-13-25. (Rule 509(c)(2)) In camera proceedings to determine whether informer should be identified--Relief to opposing party--Protective measures. If it appears in the case that an informer may be able to give testimony relevant to any issue in a criminal case or to a fair determination of a material issue on the merits in a civil case to which a public entity is a party, and the informed public entity invokes the privilege described by § 19-13-22, the court shall give the public entity an opportunity to show in camera facts relevant to determining whether the informer can in fact, supply that testimony. The showing will ordinarily be in the form of affidavits, but the court may direct that testimony be taken if it finds that the matter cannot be resolved satisfactorily upon affidavit. If the court finds there is a reasonable probability that the informer can give the testimony, and the public entity elects not to disclose his identity, in criminal cases the court on motion of the defendant or on its own motion shall grant appropriate relief, which may include one or more of the following:

(1) Requiring the prosecuting attorney to comply;

(2) Granting the defendant additional time or a continuance;

(3) Relieving the defendant from making disclosures otherwise required of him;

(4) Prohibiting the prosecuting attorney from introducing specified evidence; and

(5) Dismissing charges. In civil cases, the court may make any order the interests of justice require. Evidence submitted to the court shall be sealed and preserved to be made available to the appellate court in the event of an appeal, and the contents shall not otherwise be revealed without consent of the informed public entity. All counsel and parties are permitted to be present at every stage of proceedings under this subdivision except a showing in camera at which no counsel or party shall be permitted to be present.

19-13-33. Privileged communications concerning execution of inmate. The secretary of corrections, the warden of the penitentiary, penitentiary staff, and Department of Corrections staff may not be examined as to communications made to them concerning an execution of an inmate under chapter 23A-27A. The privilege described in this section may be claimed by the secretary of corrections, the warden of the penitentiary, penitentiary staff, Department of Corrections staff, or by any representative of any of the foregoing to be

examined and is binding on all of them. However, the secretary of corrections and the warden of the penitentiary may personally waive the privilege described in this section.

CHAPTER 22-24B SEX OFFENDER REGISTRY

22-24B-8. Information required for sex offender registration--DNA sample--Violation as felony. The registration shall include the following information which, unless otherwise indicated, shall be provided by the offender:

(1) Name and all aliases used;

(2) Complete description, photographs, fingerprints and palm prints collected and provided by the registering agency;

(3) Residence, length of time at that residence including the date the residence was established, and length of time expected to remain at that residence;

(4) The type of sex crime convicted of;

(5) The date of commission and the date of conviction of any sex crime committed;

(6) Social Security number on a separate confidential form;

(7) Driver license number and state of issuance;

(8) Whether or not the registrant is receiving or has received any sex offender treatment;

(9) Employer name, address, and phone number or school name, address, and phone number;

(10) Length of employment or length of attendance at school;

(11) Occupation or vocation;

(12) Vehicle license plate number of any vehicle owned by the offender;

(13) Information identifying any internet accounts of the offender as well as any user names, screen names, and aliases that the offender uses on the internet;

(14) A listing of all felony convictions, in any jurisdiction, for crimes committed as an adult and sex offense convictions and adjudications subject to sex offender registry

provided by the offender and confirmed by the registering agency;

(15) A description of the offense, provided by the prosecuting attorney;

(16) Acknowledgment whether the offender is currently an inmate, parolee, juvenile in department of corrections placement or under aftercare supervision, county or city jail inmate or detainee in a juvenile detention center, provided by the offender and confirmed by the administering body of the correctional facility;

(17) Acknowledgment whether the offender is subject to community safety zone restrictions, provided by the registering agency;

(18) The name, address and phone number of two local contacts, who have regular interaction with the offender and the name, address and phone number of the offender's next of kin;

(19) Passport and any document establishing immigration status, including the document type and number; and

(20) Any professional, occupational, business or trade license from any jurisdiction.

In addition, at the time of the offender's registration, the registering agency will collect a DNA sample and submit the sample to the South Dakota State Forensic Laboratory in accordance with procedures established by the South Dakota State Forensic Laboratory. The collection of DNA at the time of the registration is not required if the registering agency can confirm that DNA collection and submission to the South Dakota State Forensic Laboratory has already occurred.

Any failure by the offender to accurately provide the information required by this section is a Class 6 felony.

22-24B-15. Registration records and lists as public records--Confidentiality of victim identifying information. Any registration record collected by local law enforcement agencies pursuant to this chapter, registration lists provided to local law enforcement by the Division of Criminal Investigation, and records collected by institutions pursuant to § 22-24B-13 for those persons required to register under the provisions of §§ 22-24B-1 to 22-24B-14, inclusive, is a public record as provided in chapter 1-27.

Nothing in this section permits the release of the name or any identifying information regarding the victim of the crime to any person other than law enforcement agencies, and such victim identifying information is confidential.

22-24B-29. Summary description of offense forwarded to or developed by Division of Criminal Investigation. If any person is convicted of a sex crime as defined in § 22-24B-1 that is subject to sex offender registration requirements as defined in §§ 22-24B-2 to 22-24B-14, inclusive, the prosecuting attorney shall prepare a summary description of the offense and forward this to the Division of Criminal Investigation for inclusion on the sex offender registry.

Any person who, on July 1, 2006, is subject to sex offender registration or is subject to sex offender registration as a result of a foreign criminal conviction, may have a summary description of the offense developed by the Division of Criminal Investigation and entered on the registry, if the information is available.

The term, foreign criminal conviction, as used in this section and § 22-24B-31, means any conviction issued by a court of competent jurisdiction of another state, federal court, Indian tribe, the District of Columbia, or a commonwealth, territory, or possession of the United States which is enforceable as if the order was issued by a court in this state.

Nothing in this section allows the release of the name of the victim of the crime to any person other than law enforcement agencies, and the name of the victim is confidential.

CHAPTER 23-5 CRIMINAL IDENTIFICATION

23-5-6. Identification records made by wardens and superintendents of penal institutions. The warden or superintendent of any penal or reformatory institution in this state, the attorney general or his authorized assistants or agents, the sheriff of any county in this state, or the chief of police of any municipality in the state is hereby authorized and empowered, when in his judgment such proceeding shall be necessary for the purpose of identifying any person accused or convicted of crime, or for the purpose of preventing the escape or of facilitating the recapture of any such person, to cause to be taken or made and preserved such photographs, impressions, measurements, descriptions, and records as may in the judgment of any of said officials be deemed necessary.

23-5-7. Records for identification of prisoners--Filing and preserving in department or institution--Restrictions as to use. All photographs, impressions, measurements, descriptions, or records including confidential criminal investigative information, taken or made as provided for in § 23-5-6 shall be filed and preserved by the department or institution where made or taken and shall not be published, transferred, or circulated outside such department or institutions, nor exhibited to the public or any person or persons except duly authorized law enforcement officers unless the subject of such photograph, measurement, description, or other record becomes a fugitive from justice, or escapes from a penal institution. However, this section shall not apply to the release of information allowed pursuant to § 24-2-20.

23-5-8. Warden of penitentiary--Furnishing of identification of inmates, transmission to Division of Criminal Investigation. The warden of the penitentiary shall furnish photographs,

fingerprints, and other identifying information of all inmates received at such institution and shall transmit the same to the Division of Criminal Investigation.

23-5-10. Definition of terms. Terms used in §§ 23-5-10 to 23-5-13, inclusive, mean:

(1) "Confidential criminal justice information," criminal identification information compiled pursuant to chapter 23-5, criminal intelligence information, criminal investigative information, criminal statistics information made confidential pursuant to § 23-6-14, and criminal justice information otherwise made confidential by law;

(2) "Criminal history information," arrest information, conviction information, disposition information and correction information compiled by the attorney general pursuant to chapter 23-5, commonly referred to as a "rap sheet";

(3) "Criminal intelligence information," information associated with an identifiable individual, group, organization, or event compiled by a law enforcement agency: in the course of conducting an investigation into a criminal conspiracy, projecting a potential criminal operation, or producing an estimate of future criminal activities; or in relation to the reliability of information derived from reports of informants or investigators or from any type of surveillance;

(4) "Criminal investigative information," information associated with an individual, group, organization, or event compiled by a law enforcement agency in the course of conducting an investigation of a crime or crimes. This includes information about a crime or crimes derived from reports of officers, deputies, agents, informants, or investigators or from any type of surveillance;

(5) "Call for service," an event occurring in or near the jurisdiction of a law enforcement agency that requires law enforcement response, evaluation, action, or documentation.

23-5-11. Confidential criminal justice information not subject to inspection--Exception. Confidential criminal justice information and criminal history information are specifically exempt from disclosure pursuant to §§ 1-27-1 to 1-27-1.15, inclusive, and may be withheld by the lawful custodian of the records. Information about calls for service revealing the date, time, and general location and general subject matter of the call is not confidential criminal justice information and may be released to the public, at the discretion of the executive of the law enforcement agency involved, unless the information contains intelligence or identity information that would jeopardize an ongoing investigation. The provisions of this section do not supersede more specific provisions regarding public access or confidentiality elsewhere in state or federal law.

23-5-12. Examination of own criminal history information--Written request--Authorization of release to others--Waiver of liability. Any person may examine criminal history information filed with the attorney general that refers to that person. The person requesting such information shall supply the attorney general with a written request together with fingerprint identification. The person may also authorize the attorney general to release his criminal history information to other individuals or organizations. The attorney general may require the person to sign a waiver releasing the state, its employees or agents from any liability before releasing criminal history information.

CHAPTER 23-6 CRIMINAL STATISTICS

23-6-4. Statistical information--Compilation by director--Misdemeanor. The director shall collect and compile information, statistical and otherwise, which will, as far as practicable, present an accurate survey of the number and character of crimes committed in the state, the extent and character of delinquency, the operations of the police, prosecuting attorneys, courts and other public agencies of criminal justice, and the operations of penal and reformatory institutions, probation, parole, and other public agencies concerned with the punishment or treatment of criminal offenders. He shall include such information as may be useful in the study of crime and delinquency and the causes thereof, for the administration of criminal justice, and for the apprehension, punishment and treatment of criminal offenders. A violation of this section is a Class 2 misdemeanor.

23-6-5. Information as to particular offenders--Gathering by director--Misdemeanor. The director shall also gather such information concerning particular criminal offenders as in his judgment may be helpful to other public officials or agencies dealing with them. A violation of this section is a Class 2 misdemeanor.

23-6-8. Information received by bureau--Filing by director--Form and classification of records, preservation. The director shall file, or cause to be filed, all information received by the bureau and shall make, or cause to be made, a complete and systematic record and index thereof, to provide a convenient method of reference and consultation. As far as practicable all such records shall coincide in form and classification with those of the appropriate agency in the United States Department of Justice, and with those of similar bureaus in other states, in order to permit easy interchange of information and records. Information and records received by the bureau may not be destroyed except as provided by § 23-6-8.1.

23-6-8.1. Destruction of records of certain persons, incidents, and offenses. The director of the Bureau of Criminal Statistics may authorize the destruction of information

and records of:

(1) Persons who are dead;

(2) Persons seventy-five years of age or older unless a violation has occurred within the last ten years;

(3) Incidents that are no longer considered crimes under the laws of the State of South Dakota;

(4) Misdemeanor offenses whose final date of disposition occurred at least ten years prior to authorized destruction date.

23-6-9. Copy of available information--Furnishing to law enforcement agencies--Misdemeanor. Upon request therefor and payment of the reasonable cost, the director shall furnish a copy of all available information and of records pertaining to the identification and history of any person or persons of whom the bureau has a record, to any similar governmental bureau, sheriff, chief of police, prosecuting attorney, attorney general, or any officer of similar rank and description of the federal government, or of any state or territory of the United States or of any insular possession thereof, or of the District of Columbia, or of any foreign country, or to the judge of any court, before whom such person is being prosecuted, or has been tried and convicted, or by whom such person may have been paroled. A violation of this section is a Class 2 misdemeanor.

23-6-14. Access to files and records of bureau. The Governor, and persons specifically authorized by the director, shall have access to the files and records of the bureau. No such file or record of information shall be given out or made public except as provided in this chapter, or except by order of court, or except as may be necessary in connection with any criminal investigation in the judgment of the Governor or director, for the apprehension, identification or trial of a person, or persons, accused of crime, or for the identification of deceased persons, or for the identification of property.

CHAPTER 23-5A DNA SAMPLES

23-5A-2. Establishment of State DNA Database and State DNA Databank--Purpose--Compatibility with FBI procedures--Capabilities. There is hereby established under the administration of the South Dakota State Forensic Laboratory the State DNA Database and State DNA Databank. The South Dakota State Forensic Laboratory shall provide DNA records to the Federal Bureau of Investigation for the searching of DNA records nationwide and storage and maintenance by CODIS. The State DNA Databank shall serve as the repository for DNA samples obtained pursuant to this chapter. The State DNA Database shall be compatible with the procedures specified by the Federal Bureau of Investigation, including use of comparable test procedures, laboratory and computer equipment, supplies, and computer platform and software. The State DNA Database shall have the capability provided by computer software and procedures administered by the South Dakota State Forensic Laboratory to store and maintain DNA records related to:

(1) Crime scene evidence and forensic casework;

(2) Convicted offenders and juveniles adjudicated delinquent who are required to provide a DNA sample under this chapter;

(3) Unidentified persons or body parts;

(4) Relatives of missing persons; and

(5) Anonymous DNA profiles used for forensic validation, forensic protocol development, or quality control purposes or establishment of a population statistics database.

23-5A-22. Confidentiality of records--Disclosure prohibited. Any DNA record or DNA sample submitted to the South Dakota State Forensic Laboratory pursuant to this chapter is confidential and may not be disclosed to or shared with any person or agency unless disclosure is authorized by this chapter.

23-5A-23. Records not public. Any DNA record or DNA sample submitted to the South Dakota State Forensic Laboratory pursuant to this chapter is confidential and is not a public record under chapter 1-27.

23-5A-25. Release of record or sample for certain authorized purposes. Any DNA record or DNA sample submitted to the South Dakota State Forensic Laboratory may only be released for the following authorized purposes:

(1) For law enforcement identification purposes, including the identification of human remains, to federal, state, or local criminal justice agencies;

(2) For criminal defense and appeal purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which such defendant is charged or was convicted;

(3) If personally identifiable information is removed, for forensic validation studies, forensic protocol development or quality control purposes and for establishment or maintenance of a population statistics database, to federal, state, or local forensic laboratories or law enforcement agencies; and

(4) If ordered by the court for determination of parentage and if there is no other available DNA sample and all other reasonable opportunities to locate a known sample have been exhausted.

23-5A-26. Disclosure to unauthorized person or agency a felony--Unauthorized use or tampering a felony. Any person who knowingly or intentionally discloses any DNA record or the results of a forensic DNA analysis, to a person or agency other that one authorized to have access to such records under this chapter; or knowingly or intentionally uses or receives DNA records, or the results of a forensic DNA analysis, for purposes other than those authorized under this chapter; or knowingly or intentionally tampers or attempts to tamper with any DNA sample or the collection container without lawful authority, is guilty of a Class 5 felony.

23-5A-27. Confidentiality of software and databases used by state laboratory. The computer software and database structures used by the South Dakota State Forensic Laboratory to implement this chapter are confidential.

23-5A-28. Request for expungement--Grounds. Any person whose DNA record or DNA profile has been included in the State DNA Database in accordance with this chapter may request expungement on the grounds that the arrest that led to the inclusion of the person's DNA record or DNA profile has not resulted in a felony charge within one year; has been resolved by a dismissal, acquittal, or misdemeanor conviction; or has not resulted in a felony conviction; or the conviction or delinquency adjudication on which the authority for including that person's DNA record or DNA profile was based has been reversed and the case dismissed.

23-5A-29. Expungement of record--Receipt of court order--Exception. Upon receipt of written request for expungement; certified copy of the final court order reversing and dismissing the conviction or delinquency adjudication; and any other information necessary to ascertain the validity of the request, the South Dakota State Forensic Laboratory shall expunge all DNA records and identifiable information in the database pertaining to the person and destroy the DNA sample from the person, unless the South Dakota State Forensic Laboratory determines that the person has otherwise become obligated to submit a DNA sample.

23-5A-30. Expungement not required if certain other evidence would be destroyed. The South Dakota State Forensic Laboratory is not required to destroy an item of physical evidence obtained from a sample if evidence relating to another person would thereby be destroyed.

23-5A-31. Failure to expunge not grounds for invalidation. Any identification, warrant, probable cause to arrest, or arrest based upon a database match is not invalidated due to a failure to expunge or a delay in expunging records

---

CHAPTER 23A-27 SENTENCE AND JUDGMENT

23A-27-17. Sealing of records on discharge of probationer--Effect of order--Future statements by defendant as to conviction. Upon the discharge and dismissal of a person pursuant to § 23A-27-14, a court shall order that all official records, other than the

nonpublic records to be retained by the Division of Criminal Investigation, be sealed along with all records relating to the person's arrest, indictment or information, trial, finding of guilt, and dismissal and discharge. The effect of such order is to restore such person, in the contemplation of the law, to the status he occupied before his arrest or indictment or information. No person as to whom such order has been entered shall be held thereafter under any provision of any law to be guilty of perjury or of giving a false statement by reason of his failure to recite or acknowledge such arrest, indictment or information, or trial in response to any inquiry made of him for any purpose.

CHAPTER 23A-27A CAPITAL PUNISHMENT

23A-27A-31.2. Confidentiality of identity of person administering intravenous injection--Violation as misdemeanor. The name, address, qualifications, and other identifying information relating to the identity of any person administering the intravenous injection under chapter 23A-27A are confidential. Disclosure of the foregoing information may not be authorized or ordered. Disclosure of confidential information pursuant to this section concerning the execution of an inmate under chapter 23A-27A is a Class 2 misdemeanor.

23A-27A-37. Secrecy of execution time--Disclosure as misdemeanor. Prior to the announcement required in § 23A-27A-17, the scheduled day and time fixed by the warden for the execution shall be kept secret and in no manner divulged except privately to the persons invited or requested to be present as provided by §§ 23A-27A-32, 23A-27A-34, 23A-27A-34.1, and 23A-27A-34.2. It is a Class 2 misdemeanor for any person to divulge such invitation to anyone or in any manner disclose the scheduled day and time of the execution prior to the announcement required in § 23A-27A-17.

CHAPTER 23A-28C CRIME VICTIMS' ACT

23A-28C-2. Notice of rights--Victim's response--Duty of Department of Corrections--Confidentiality. At the commencement of a criminal proceeding subject to the terms of this chapter, the prosecutor, by first class mail, shall advise the victim of the rights set forth in this chapter. In order to take advantage of such rights, the victim shall advise the prosecutor of the desire to participate. A victim may choose to participate only in certain enumerated phases of the proceedings. A victim wishing to participate shall advise the prosecutor or the Department of Corrections of the place where notifications required under

this chapter are to be made, and of any changes in the place of notification. A prosecutor receiving notification of a victim's wish to participate shall keep record of that notification and most recent place of notification through the time of the defendant's final discharge from the criminal justice system. If the defendant is sentenced to the state prison system, the prosecutor shall forward the information to the Department of Corrections and the Department of Corrections shall keep record of the request for notification and the most recent place of notification until the defendant's final discharge from prison and parole. The request for notification and the place of notification is confidential and may not be disclosed to the defendant.

23A-28C-9. Notification of immediate family. No person, other than in the performance of official duties, may disclose the identity and biographical information concerning a victim of a crime of violence or of a violation of § 22-22-7 until reasonable efforts have been made to notify one of the immediate family.

CHAPTER 23A-3 (RULE 4.1) ARREST

23A-3-26. Definition of expungement. Terms used in §§ 23A-3-27 to 23A-3-33, inclusive, mean:

(1) "Expungement," the sealing of all records on file within any court, detention or correctional facility, law enforcement agency, criminal justice agency, or Department of Public Safety concerning a person's detection, apprehension, arrest, detention, trial or disposition of an offense within the criminal justice system. Expungement does not imply the physical destruction of records.

23A-3-27. Motion for expungement of arrest record. An arrested person may apply to the court that would have jurisdiction over the crime for which the person was arrested, for entry of an order expunging the record of the arrest after one year from the date of any arrest, if no accusatory instrument was filed, or at any time after an acquittal.

23A-3-28. Service of motion--Fee. At least fourteen days before any hearing on a motion for expungement, a copy of the motion shall be served upon the office of the prosecuting attorney who prosecuted the crime or violation, or who had authority to prosecute the charge if there was no accusatory instrument filed. The prosecuting attorney may contest the motion in writing and at the hearing on the motion.

When a defendant or arrested person makes a motion under this section, the defendant or arrested person shall pay to the clerk of courts in the county where the motion is filed a fee equal to the filing fee for a civil action. If the defendant or arrested person establishes to

the court's satisfaction that the person is indigent and unable to pay the fee, the court may waive the filing fee.

23A-3-29. Hearing on motion for expungement. The court may fix a time and place for a hearing on the motion unless waived by the defendant, arrested person, prosecuting attorney, and victim. The court may require the filing of such affidavits and may require the taking of such evidence as it deems proper.

23A-3-30. Order of expungement. The court may enter an order of expungement if satisfied that the ends of justice and the best interest of the public as well as the defendant or the arrested person will be served by the entry of the order.

23A-3-31. Report to Division of Criminal Investigation--Retention and use of nonpublic records--Sealing of records. Any order of expungement shall be reported to the Division of Criminal Investigation pursuant to chapters 23-5 and 23-6. The court shall forward a nonpublic record of disposition to the Division of Criminal Investigation which shall be retained solely for use by law enforcement agencies, prosecuting attorneys, and courts in sentencing the defendant or arrested person for subsequent offenses.

As part of any order of expungement, the court shall order that all official records, other than the nonpublic records to be retained by the Division of Criminal Investigation, be sealed along with all records relating to the defendant or arrested person's arrest, detention, indictment or information, trial, and disposition.

23A-3-32. Effect of order of expungement. The effect of an order of expungement is to restore the defendant or arrested person, in the contemplation of the law, to the status the person occupied before the person's arrest or indictment or information. No person as to whom an order of expungement has been entered shall be held thereafter under any provision of any law to be guilty of perjury or of giving a false statement by reason of the person's failure to recite or acknowledge the person's arrest, indictment or information, or trial in response to any inquiry made of the person for any purpose.

23A-3-33. No time limitation for making application. A court may issue an order of expungement for arrests that occurred before, as well as those that occurred after, July 1, 2010. There is no statute of limitation for making an application.

CHAPTER 26-7A JUVENILE COURT

26-7A-27 Police records of children taken into temporary custody--Confidentiality.
26-7A-28 Release of information on identity of child prohibited except by court order or when child adjudicated delinquent offender.
26-7A-29 Release of information to persons, agencies, or facilities with legitimate interest in child.
26-7A-36 Hearings closed unless court compelled otherwise--Exceptions.
26-7A-37 Persons authorized to inspect or receive copies of records of court proceedings.
26-7A-38 Protection of identity of witnesses--Violation creates cause of action for civil damages--Contempt.
26-7A-39 Compulsory process for attendance of defense witnesses. exceptional circumstances.
26-7A-78 Deposition enclosed, sealed, and endorsed--Transmitted to county clerk. a criminal conviction.

26-7A-27. Police records of children taken into temporary custody--Confidentiality. The records of law enforcement officers and agencies concerning all children taken into temporary custody or issued a summons or citation under this chapter or chapter 26-8A, 26-8B, or 26-8C shall be maintained separately from the records of arrest and any other records regarding detention of adult persons. The records concerning children, including their names, may not be inspected by or disclosed to the public except:

(1) By order of the court;

(2) If the court orders the child to be held for criminal proceedings, as provided in chapter 26-11;

(3) If there has been a criminal conviction and a presentence investigation is being made on an application for probation; or

(4) Any child or the child's parent or guardian may authorize the release of records to representatives of the United States Military for the purpose of enlistment into the military service.

26-7A-28. Release of information on identity of child prohibited except by court order or when child adjudicated delinquent offender. No fingerprint, photograph, name, address, or other information concerning the identity of any child taken into temporary custody or issued a summons under this chapter or chapter 26-8A, 26-8B, or 26-8C may be released or transmitted to the Federal Bureau of Investigation or any other person or agency except in the following instances:

(1) To the person or party specifically authorized by order of the court; and

(2) To courts, law enforcement agencies, prosecuting attorneys, court services officers, and the Department of Social Services if the child is an adjudicated delinquent offender.

Information regarding an alleged, apparent, or adjudicated abused or neglected child may be released only in accordance with § 26-8A-13.

26-7A-29. Release of information to persons, agencies, or facilities with legitimate interest in child. Notwithstanding §§ 26-7A-27 and 26-7A-28, information concerning children may be released, pursuant to an order of the court, to persons or agencies who have a legitimate interest in the child, to the child's parents, guardian, or custodian, or to the child's attorney. The Department of Social Services may release information pursuant to provisions of § 26-8A-13 regarding apparent, alleged, or adjudicated abused or neglected children. Any correctional or detention facility may release information concerning any child to any other correctional or detention facility that has a legitimate interest in the child.

26-7A-36. Hearings closed unless court compelled otherwise--Exceptions. All hearings in actions under this chapter and chapter 26-8A, 26-8B, or 26-8C are closed unless the court finds compelling reasons to require otherwise. However, all pleadings and hearings shall be open and a matter of public record if a juvenile is summoned into court for an offense which if committed by an adult would constitute a crime of violence as defined in subdivision 22-1-2(9) or a crime involving a drug offense in violation of § 22-42-2 or 22-42-3, and at the time of the offense the juvenile was sixteen years of age or older.

26-7A-37. Persons authorized to inspect or receive copies of records of court proceedings. Records of court proceedings, including reports of the Department of Social Services, records and reports of court services officers, clinical studies, and evaluation reports, under this chapter and chapters 26-8A, 26-8B, and 26-8C shall be open to inspection by or disclosure to the child's parents, guardian, or custodian and by other respondent parties involved in the proceedings, their attorneys, the child's attorney and by any department or agency having custody of the child.

Pursuant to court order, records of court proceedings may be inspected by or disclosed to the child, by parties having a legitimate interest in the proceedings and by parties conducting pertinent research studies.

26-7A-38. Protection of identity of witnesses--Violation creates cause of action for civil damages--Contempt. The name, picture, place of residence, or identity of any child, parent, guardian, custodian, or any person appearing as a witness in proceedings under this chapter or chapter 26-8A, 26-8B, or 26-8C may not be published or broadcast in any news media or given any other publicity, unless for good cause it is specifically permitted by order of the court. Violation of this section creates a cause of action for civil damages on behalf of the child and is subject to the same punishment as contempt of court.

26-7A-78. Deposition enclosed, sealed, and endorsed--Transmitted to county clerk. A deposition taken pursuant to this section shall be enclosed, sealed, and endorsed with the title of the action and the name of the officer taking the deposition. The officer taking the deposition shall address and transmit the deposition to the clerk of courts of the county where the action is being conducted. The deposition shall remain under seal until it is opened by the clerk of courts pursuant to the order of the court, the request of any party to the action or attorney for the party, or the request of the state's attorney.

26-7A-106. Proceedings not admissible in criminal or civil action against child. No adjudication, disposition, or evidence given in any proceedings under this chapter or chapter 26-8A, 26-8B, or 26-8C is admissible against a child in any criminal, civil, or other proceeding, except in subsequent proceedings under this chapter and related chapter 26-8C regarding the delinquency of the same child and in subsequent criminal proceedings concerning the same child for sentencing purposes.

26-7A-113. Sealing records in action involving abused or neglected child--Inspection. In any action involving an abused or neglected child, the records and files of the court may be sealed by court order issued on the court's own motion or on the petition of any party to the action after the termination or completion of the action in all respects and after the expiration of the time for all appeals. If parental rights were terminated, the records and files of the court may not be sealed until adoption proceedings concerning the child have been completed or the court specifically orders the records and files sealed on the court's finding, based on information received by the court from the Department of Social Services, that adoption of the child is improbable. After the court records and files relating to the

action concerning the abused or neglected child are sealed, inspection of the records and files may thereafter be permitted by the court only on petition by the guardian, guardian ad litem, or attorney for the child who is the subject of the action, by respondent parents whose parental rights have not been terminated or by the Department of Social Services. Before allowing inspection of sealed records and files, the court shall find that the inspection is in keeping with the best interests of the child.

26-7A-114. Sealing records in action involving child in need of supervision--Inspection. In any action involving a child in need of supervision, the records and files of the court may be sealed by court order issued on the court's own motion or on the petition of any party to the action after the termination or completion of the action in all respects, after the expiration of the time for all appeals and after the unconditional release of the child from the court's jurisdiction. After the records and files are sealed, inspection of them may thereafter be permitted by the court only on petition by the state's attorney, guardian, guardian ad litem, or attorney for the child who is the subject of the action or by the respondent parents or a court services officer. Before allowing inspection of sealed records and files, the court shall find that the inspection is in keeping with the best interests of the child.

26-7A-115. Sealing records in action involving delinquent child--Inspection. In any action involving a delinquent child, the records and files of the court may be sealed by a court order issued on the court's own motion or on the petition of the child or the child's parents. However, no such petition may be filed and considered by the court until after one year from the date of the child's unconditional release from the court's jurisdiction or the discharge of the child by the Department of Corrections, whichever date is later. Upon the filing of the petition, the court shall set a date for hearing and shall notify the state's attorney and any other party who the court believes may have relevant information about the delinquent child. The court may order sealed all of the court's records and files and the records and files in the custody or under the control of any other agency or official if at the hearing on the petition to seal the court finds:

(1) The delinquent child has not been adjudicated as a delinquent under this chapter or chapter 26-8C since the termination of the court's jurisdiction of the child or the discharge of the child by the Department of Corrections;

(2) No proceeding involving the delinquent child concerning a felony, a sexual contact offense, a misdemeanor involving moral turpitude or a petition under this chapter or chapter 26-8C is pending or is being instituted against the child; and

(3) The rehabilitation of the delinquent child has been attained to the satisfaction of the court.

26-7A-116. Distribution of copies of order sealing records--Inspection of sealed records. If the court orders the sealing of the records and files pursuant to § 26-7A-113, 26-7A-114, or 26-7A-115, copies of the sealing order shall be sent to each agency or official named in the order. Subsequent inspection of the sealed records may thereafter be permitted by the court only on petition by the child who is the subject of the record, the state's attorney, or court services officers. The court may permit inspection of the sealed records and files for use by the court in other actions or proceedings under this chapter or chapter 26-8C and for subsequent criminal proceedings for sentencing purposes. Nothing in this chapter prohibits the custodian of records or files from inspecting or accessing the

custodian's records or files as may be necessary for the discharge of the custodian's official duties in the absence of an order from the court.

26-7A-120. Confidentiality of records. Records prepared or maintained by court services officers are confidential. However, such records may be inspected by, or disclosed to, justices, judges, magistrates, and employees of the Unified Judicial System in the course of their duties and to persons specifically authorized by order of the court.

CHAPTER 26-8A PROTECTION OF CHILDREN FROM ABUSE OR NEGLECT

26-8A-8. Oral report of abuse or neglect--To whom made--Response report. The reports required by §§ 26-8A-3, 26-8A-6, and 26-8A-7 and by other sections of this chapter shall be made orally and immediately by telephone or otherwise to the state's attorney of the county in which the child resides or is present, to the Department of Social Services or to law enforcement officers. The state's attorney or law enforcement officers, upon receiving a report, shall immediately notify the Department of Social Services. Any person receiving a report of suspected child abuse or child neglect shall keep the report confidential as provided in § 26-8A-13, except as otherwise provided in chapter 26-7A or this chapter.

The person receiving a report alleging child abuse or neglect shall ask whether or not the reporting party desires a response report. If requested by the reporting person, the Department of Social Services or the concerned law enforcement officer shall issue within thirty days, a written acknowledgment of receipt of the report and a response stating whether or not the report will be investigated.

26-8A-10.1. Notice to child's parents of determination of abuse or neglect--Contents--Confidentiality. If an investigation by the Department of Social Services determines that abuse or neglect has occurred, the department shall make reasonable efforts to inform each of the child's parents of the determination with due regard given to the rights of the subject of the report pursuant to § 26-8A-11. The information shall only include identification of the provisions of § 26-8A-2 which constituted the basis for the determination that abuse or neglect occurred. This provision does not limit the department in providing services to a parent who is the subject of the report. A notice of the report shall be sent, by certified mail, to any parent who is not the subject of the report at the parent's last known address. The information shall be maintained confidential by the parent pursuant to § 26-8A-13.

26-8A-11.1. Request for a hearing to release name of complainant in unsubstantiated investigation. Within thirty days after the notice of the determination of an unsubstantiated investigation by the Department of Social Services, the person who is the subject of the investigation may request an administrative hearing to determine whether the report was made with malice and without reasonable foundation and whether the name of the complainant should be released to the subject of the investigation. Within twenty days of receiving the request, an administrative hearing officer shall notify the complainant by mail that a request to release the complainant's name has been made and set a time and date for a hearing. The complainant shall be afforded the opportunity to be heard prior to any determination by the hearing officer to release the name. The complainant may appear at the hearing in person or through counsel or may submit written objections to the request in lieu of appearance. Any written objections or other information that may reveal the name of the complainant shall be sealed and available only to the administrative hearing officer. The administrative hearing officer shall determine within ninety days of the final date of the hearing whether the report was made maliciously and without reasonable foundation and whether release of the complainant's name would be likely to endanger the complainant's life or safety. The administrative hearing officer shall issue such a finding in a written report. The report may not disclose the name of the complainant or other identifying information. If the administrative hearing officer determines that the report was made with malice and without reasonable foundation and that release of the complainant's name is not likely to endanger the complainant's life or safety, the officer shall order the department to release the name of the complainant thirty days after issuing such finding. If the administrative hearing officer determines that the report was not made with malice or that the report was made with reasonable foundation or that release of the complainant's name is likely to endanger the life or safety of the complainant, the name of the complainant may not be disclosed. Decisions of the department under this section are administrative decisions subject to review under chapter 1-26. If a decision of the department under this section is appealed under chapter 1-26, the identity of the complainant shall remain confidential until a final court order requiring the release of the complainant's name.

26-8A-13. Confidentiality of abuse or neglect information--Violation as misdemeanor--Release to certain parties. All investigative case records and files relating to reports of child abuse or neglect are confidential, and no disclosure of any such records, files, or other information may be made except as authorized in chapter 26-7A or this chapter. Any person who knowingly violates the confidential nature of the records, files, or information is guilty of a Class 1 misdemeanor. The Department of Social Services may release records, files, or other information to the following parties upon receipt of a request showing that it is necessary for the parties to have such information in the performance of official functions relating to child abuse or neglect:

(1) The attorney general, the state's attorneys, law enforcement agencies, protective services workers, and judges of the courts investigating reports of known or suspected child abuse or neglect;

(2) The attorney or guardian ad litem of the child who is the subject of the information;

(3) Public officials or their authorized representatives who require the information in connection with the discharge of official duties;

(4) Institutions and agencies that have legal responsibility or authorization to care for, treat, or supervise a child who is the subject of the information or report;

(5) An adoptive parent of the child who is the subject of the information or report;

(6) A foster parent, kinship provider, or prospective adoptive parent who is or may be caring for a child in the custody of the Department of Social Services who is the subject of the information or report;

(7) A state, regional, or national registry of child abuse and neglect cases and courts of record of other states;

(8) A validly appointed and registered child protection team under § 26-8A-17;

(9) A physician caring for a child who is suspected or found to be abused or neglected;

(10) State hearing examiners and any person, or the legal representative of any person, who is the subject of the report for purposes directly related to review under § 26-8A-11; and

(11) A person eligible to submit an adoptive home study report under § 25-6-9.1 or 26-4-15. However, the information may only be released for the purpose of screening applicants.

Information received by an authorized receiving party shall be held confidential by the receiving party. However, the court may order the release of the information or any portion of it necessary for determination of an issue before the court.

Upon written request, the Department of Social Services shall release findings or information regarding the abuse or neglect of a child that resulted in a fatality or near fatality of the child unless the release of the findings or information would jeopardize a pending criminal investigation or proceeding. The findings or information to be released shall relate to the acts of child abuse or neglect that caused the fatality or near fatality of the child. However, the identity of the child may never be released. For the purpose of this chapter, near fatality means an act that, as certified by a physician, placed the child in serious or critical condition.

26-8A-13.1. Certain child protection records to be provided to the court, court services, state's attorney, or agencies--Discovery--Fees. Notwithstanding the provisions of § 26-8A-13, or any other statute to the contrary, in any case that a child is under the jurisdiction of the court pursuant to chapter 26-8B or 26-8C, upon a request for information, the Department of Social Services shall, with due regard to any federal laws or regulations, including the Health Information Portability and Accountability Act of 1996, as amended to January 1, 2007, the Family Educational Rights and Privacy Act, as amended to January 1, 2007, and the federal rules governing the confidentiality of alcohol and drug abuse patient records pursuant to 42 C.F.R. Part 2, as amended to January 1, 2007, in the following instances:

(1) Conduct a child abuse and neglect central registry check and provide the results to the court, court services, or the state's attorney to determine the appropriateness

of returning a child to the parents or placing the child with another caretaker at any time during the pendency of the proceedings;

(2) For a child committed to the Department of Corrections, conduct a child abuse and neglect central registry check and provide the results to the Department of Corrections for purposes of determining the appropriateness of returning a child to the parents or placing the child with another caretaker; and

(3) For a child committed to the Department of Corrections, release copies of, or the equivalent to, the child's: request for services history summary, initial family assessments, court reports, and family service agreements to the Department of Corrections for treatment planning purposes.

Upon receipt of an order of the court, the Department of Social Services shall make its child protection services file related to the child or the child's parents and siblings available to the court, court services, or the state's attorney with the exception of information protected by the Health Information Portability and Accountability Act of 1996, as amended to January 1, 2007, the Family Educational Rights and Privacy Act, as amended to January 1, 2007, and the federal rules governing the confidentiality of alcohol and drug abuse patient records pursuant to 42 C.F.R. Part 2, as amended to January 1, 2007. Under no circumstances may the court order the release of information pertaining to pending abuse or neglect investigations.

The information released under this section is discoverable to the parties under the provisions of chapter 26-7A, but is otherwise confidential. However, the court, court services, or the Department of Corrections may release the information in their possession or any portion necessary to institutions and agencies that have legal responsibility or authorization to care for, treat, or supervise a child. The attorneys for the child and respondents may review the records with the child and the respondents but may not copy or release copies of the records. A pro se litigant is entitled to review the records but may not copy or release copies of the records.

The Department of Social Services shall impose reasonable fees for reproduction of its records released under this section. The Department of Social Services shall promulgate rules pursuant to chapter 1-26 for any fee imposed for records reproduction.

26-8A-16. Photographs, videotapes, or other images, and medical examinations taken without consent--Disposition. Any person who receives a report under § 26-8A-3 may take or cause to be taken color photographs, videotapes, or other images of the areas of trauma visible on a child who is the subject of the report and may require a radiological or other medical examination or testing of the child without the consent of the child's parents, guardian, or custodian. All photographs, videotapes, or other images taken pursuant to this section shall be taken by a law enforcement official, the Department of Social Services, or a person authorized by a law enforcement official or the department. All photographs, videotapes, other images, X rays, and test results, or copies of them, shall be sent to the appropriate law enforcement agency or state's attorney or to the Department of Social Services. These photographs, videotapes, and other images need not be made a part of the child's medical or hospital records. Any photograph, videotapes, or other image in the possession of the Department of Social Services shall be destroyed by the Department of Social Services if no criminal prosecution or civil action is initiated within three years of the date that such material was received by the Department of Social Services.

26-11A-27. Powers and duties of monitor. The monitor created in § 26-11A-25 shall:

(1) Investigate incidents of abuse or neglect of such individuals within the juvenile corrections facilities, if the incidents are reported to the monitor or if there is reasonable suspicion to believe that the incidents occurred;

(2) Access any individual in the custody or care of juvenile corrections facilities and any employee in the employ of the State of South Dakota or any of its political subdivisions;

(3) Access any records of or relating to any individual in the custody or care of juvenile facilities;

(4) Provide a semi-annual report to the Governor, the Legislature, the Corrections Commission established by § 1-15-1.13, the secretary of the Department of Human Services, and the secretary of the Department of Corrections. The report shall contain the activities of the monitor for the six-month period immediately prior to the report. Activities shall reflect the number of referrals to the monitor, the number of investigations completed, a brief description of any investigation that resulted in a finding of abuse or neglect, and a summary of other activities performed by the monitor;

(5) Provide training and assistance to employees of the Department of Corrections in areas within the scope of the monitor's position;

(6) Review Department of Corrections' policies dealing with juvenile's rights to ensure compliance with federal and state laws, rules, and policy;

(7) Provide reasonable notification of the existence and role of the monitor to all individuals in the custody or care of a juvenile corrections facility and the custodial parent or guardian;

(8) Submit a confidential addendum to each semiannual report to the Government Operations and Audit committee created in § 2-6-2, the Governor, the secretary of the Department of Human Services, and the secretary of the Department of Corrections. This addendum shall contain a description of each case investigated, the specific findings and recommendations of the juvenile corrections monitor, and the Department of Corrections' response to the recommendations.

26-11A-30. Disclosure of identities of juveniles or others requesting assistance not required--Identity of person reporting to monitor to remain confidential. For purposes of any audit, report, evaluation, or public testimony that may be permitted or required under §§ 26-11A-24 to 26-11A-33, inclusive, no disclosure of the identity of, or any other

personally identifiable information related to, any juvenile or any individual requesting assistance under §§ 26-11A-24 to 26-11A-33, inclusive, shall be required. The identity of the person making a report to the monitor shall be kept confidential.

26-11A-33. Identities of persons or agencies reporting to monitor to remain confidential. The identity of the juvenile and of any person or agency making a report to the monitor shall be kept confidential.

CHAPTER 26-16 COUNTY INTERDISCIPLINARY CHILD INFORMATION TEAMS

26-16-4. Information sharing in serving child for specified purposes--Confidentiality. The county interdisciplinary child information team and the written agreement shall facilitate the exchange and sharing of information that one or more team members may be able to use in serving a child in the course of their professions, specialities, interests, or occupations for the purpose of holding each child accountable, ensuring the safety of the child and the community, and providing early intervention to avert more serious problems. Information regarding any child that a team member supplies to other team members is confidential and may not be disseminated beyond the team.

26-16-5. Terms of written agreement--Filing. The terms of the written agreement shall provide for the rules under which the team will operate, the method by which information will be shared, distributed, and managed, the means by which the confidentiality of the information will be safeguarded, and any other matters necessary to the purpose and functions of the team. The terms of the written agreement shall also provide how the team will coordinate its efforts with child protection teams as provided in § 26-8A-17 and local interagency teams, if any, as provided in § 27A-15-54. The written agreement shall be filed with the county auditor.

26-16-6. Education records. To the extent that the county interdisciplinary child information team is involved in a proceeding that is held prior to adjudication by a court, the team satisfies the requirements of 20 U.S.C. 1232g(b)(1)(E)(ii)(I) of the Family Educational Rights and Privacy Act of 1974. South Dakota school districts may release education records to the team. The terms of the written agreement, as provided for in § 26-16-5, shall include a requirement that the officials and authorities to whom the information is disclosed certify in writing to the school district that is releasing the education records that the education records or information from the education records will not be disclosed to any other party without the prior written consent of the parent or guardian of the student.

CHAPTER 27A-11A HEARINGS PROCEDURE

27A-11A-3. Filing of board papers with clerk of courts--Confidentiality and access. The chairman or acting chairman of the board of mental illness shall cause to be filed in the office of the clerk of courts all papers and any other records of proceedings connected with any inquest of the board, and properly belonging to his office with all notices, reports, and other communications. The clerk of courts shall keep separate books in which to record the proceedings of the board, and his entries shall be sufficiently full to show, with the papers filed, a complete record of the findings, orders, and transactions of the board.

All records of proceedings under this title shall be subject to the confidentiality and access provisions of § 27A-12-25 et seq. Any such records regarding a person who is released prior to or directly following the completion of a hearing provided for in § 27A-10-8 shall be sealed upon such release and shall be opened only by court order of the circuit court.

CHAPTER 27A-12 CARE, TREATMENT, AND RIGHTS OF PATIENTS WITH MENTAL ILLNESS

27A-12-25. Individual records required--Contents--Confidentiality. A complete statistical and medical record shall be kept current for each person receiving mental health services, or being otherwise detained under this title. The record shall include information pertinent to the services provided to the person, pertinent to the legal status of the recipient, required by this title or other provision of law, and required by rules or policies. The material in the record shall be confidential in accordance with the provisions of this title.

27A-12-25.1. Information closed to public inspection--Sealed upon termination of proceedings. Any information acquired by a peace officer pursuant to his authority under this title regarding any person subject to any proceedings under this title shall not be open to public inspection, and any records regarding such person shall be sealed upon the termination of proceedings for which the information was acquired, and shall be opened only by order of the circuit court.

27A-12-26. Confidentiality of information acquired in course of providing mental health services. Information in the record of a person, and other information acquired in the course of providing mental health services to a person, shall be kept confidential and are not open to public inspection. The information may be disclosed outside the center, department, mental health program, or inpatient facility, whichever is the holder of the record, only if the holder of the records and the person, his parents if he is a minor or his guardian, consent or, in the absence of such consent, in the circumstances and under the conditions set forth in §§ 27A-12-25 to 27A-12-32, inclusive, and in conformity with federal law.

27A-12-26.1. Access to own records--Exceptions--Confidentiality following discharge. A person has the right to access, upon request, to his mental health records. However, the person may be refused access to:

(1) Information in such records provided by a third party under assurance that such information remain confidential; and

(2) Specific material in such records if the qualified mental health professional responsible for the mental health services concerned has made a determination in writing that such access would be detrimental to the person's health. However, such material may be made available to a similarly licensed qualified mental health professional, selected by the person; and such professional may, in the exercise of professional judgment, provide such person with access to any or all parts of such material or otherwise disclose the information contained in the material to such person.

The rights to confidentiality of and access to records as provided in §§ 27A-12-25 to 27A-12-32, inclusive, shall remain applicable to records pertaining to such person after the person's discharge.

27A-12-27. Obligation to disclose confidential information. If requested, information shall be disclosed:

(1) Pursuant to orders or subpoenas of a court of record or subpoenas of the Legislature;

(2) To a prosecuting or defense attorney or to a qualified mental health professional as necessary for him to participate in a proceeding governed by this title;

(3) To an attorney representing a person who is presently subject to the authority of this title or who has been discharged when that person has given his consent;

(4) If necessary in order to comply with another provision of law;

(5) To the department if the information is necessary to enable the department to discharge a responsibility placed upon it by law; or

(6) To a states attorney or the attorney general for purpose of investigation of an alleged criminal act either committed by or upon a human services center patient while a patient of the center.

27A-12-30. Released information approved by administrator--Record of release. Any release of information by the holder of the record shall be approved by the administrator or facility director holding the records. The holder of the record shall keep a record of any information released, to whom, the date it was released and the purpose for such release.

27A-12-31. Identity of patient protected in disclosing information--Disclosure limited by germaneness. If information is disclosed, the identity of the individual to whom it pertains shall be protected and may not be disclosed unless it is germane to the authorized purpose for which disclosure was sought.

27A-12-32. Disclosure by recipient of confidential information. Any person receiving confidential information pursuant to § 27A-12-25 shall disclose the information to others

only to the extent consistent with the authorized purpose for which the information was obtained.

CHAPTER 27B-8 CARE, TREATMENT AND RIGHTS OF RESIDENTS IN FACILITIES FOR THE DEVELOPMENTALLY DISABLED

27B-8-46. Records confidential--Disclosure. All records kept pursuant to this chapter are confidential and not open to public inspection. The information may be disclosed only in the circumstances and under the conditions set forth in §§ 27B-8-47 to 27B-8-49, inclusive.

27B-8-47. Disclosure of information to certain persons. If the community service provider or facility and the person with a developmental disability and the person's parent, if a minor, or the person's guardian consent, information may be disclosed to providers of supports and services to the person with a developmental disability, or to the person with a developmental disability, or to any other person or agency, if, in the judgment of the community service provider or facility, the disclosure would not be detrimental to the person with a developmental disability.

27B-8-48. Identity of person to be protected. If information is disclosed, the identity of the person to whom it pertains shall be protected and may not be disclosed unless it is germane to the authorized purpose for which disclosure was sought. If practicable, no other information may be disclosed unless it is germane to the authorized purpose for which disclosure was made.

27B-8-49. Further disclosure of information. Any person receiving information made confidential by § 27B-8-47 shall disclose the information to others only to the extent consistent with the authorized purpose for which the information was released.

CHAPTER 28-1 STATE DEPARTMENT OF SOCIAL SERVICES

28-1-80 Confidentiality of investigative records and files of program.

28-1-29. Public assistance records confidential--Exceptions. Any application or record concerning any applicant for, or recipient of, public assistance provided under the laws of this state through the Department of Social Services is confidential except:

(1) For inspection by any person duly authorized by this state or the United States in connection with the person's official duties;

(2) For the purpose of fair hearings as provided by law.

28-1-45.1. Records required--Improper use of names or information concerning persons applying for assistance. The adult services and aging programs shall keep such records as may be required by law or federal regulations. All applications and records concerning any applicant or recipient are confidential. Except for purposes directly connected with the administration of the adult services and aging program and in accordance with the rules of the department, no person may solicit, disclose, or make use of, or authorize, knowingly permit, participate in, or acquiesce in the use of any lists or names of, or any information concerning, persons applying for or receiving public assistance, derived from the records, papers, files, or communications of the department acquired in the course of the performance of official duties.

28-1-45.2. Use of information--Publication of names of applicants and recipients prohibited. The use or disclosure of information concerning applicants and recipients is limited to:

(1) Any person authorized by the secretary in connection with the secretary's official duties, if the official duties are directly connected with the administration of the adult services and aging program;

(2) Any purpose directly connected with the adult services and aging program, including disclosure by the department of information and documents, alleged violator, police department, prosecutor's offices, the attorney general's office, or any other state, county, or federal agency engaged in the detection, investigation, or prosecution of violations of applicable state, county, and federal laws or regulations regarding all aspects of theft, fraud, deception, or overpayment in connection with any aspect of the adult services and aging program. However, disclosure by recipient agencies and personnel is permitted under this section to the extent reasonably necessary to carry out the functions for which the information was provided;

(3) Federal agencies responsible for the administration of federally assisted programs, which provide assistance in cash or in kind.

Any publication of lists or names of applicants and recipients is prohibited.

28-1-45.3. Promulgation of rules--Use of information within scope of employment--Confidential records--Inspection. The department shall promulgate rules pursuant to chapter 1-26 as may be necessary to prevent improper acquisition or use of confidential information. Any information secured pursuant to §§ 28-1-45.1 to 28-1-45.5, inclusive, by

officials or employees may be used in connection with their official duties or within the scope and course of employment, but not otherwise, and shall be kept in confidential records or files, which are not subject to any other law permitting inspection of public records. The secretary shall determine whether such inspection is in connection with such official duties or within the scope or course of such employment.

28-1-45.4. Use of records by other agency limited. The use of records, and other communications of the department or its agents by any other agency or department of government to which they may be furnished is limited to the purposes for which they are furnished.

28-1-45.5. Release of confidential information by written waiver-Exception. Except for adult protective services cases, confidential information shall be released if requested by specific written waiver of the applicant or recipient concerned.

28-1-51. Rules for protection of confidential information. The secretary of social services may adopt reasonable and necessary rules to protect records and confidential information required by statutory law to be held confidential.

28-1-68. Confidentiality of enforcement services applications and records. All applications and records concerning any applicant for child and spousal support enforcement services are confidential except:

(1) For inspection by persons authorized by this state or the United States in connection with their official duties;

(2) For the purpose of fair hearings provided by law.

28-1-78. Program of recoveries and fraud investigations--Debt collection and fraud allegation investigations--Authority of investigators. The department shall have a program of recoveries and fraud investigations to collect debts owed the department and to investigate allegations of fraud in all department assistance programs. Any fraud investigator for this program may:

(1) Initiate and conduct any investigation if the program has cause to believe that a fraudulent act has been committed by a recipient of assistance from department programs;

(2) Review any report or complaint of an alleged fraudulent act to determine whether such report requires further investigation and conduct such investigation;

(3) Obtain access to any record related to residence, household composition, employment, finances and resources, and medical records as authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), PL 104-199, as amended through January 1, 2005, to assist in investigation of an alleged fraudulent act and may require by administrative subpoena the production of any book, record, or other information; and

(4) Cooperate with federal, state, and local law enforcement, prosecuting attorneys, and the attorney general in the investigation and prosecution of any fraudulent act where public assistance has been granted or applied for under the welfare laws of this

state.

28-1-80. Confidentiality of investigative records and files of program. All investigative records and files of the program established pursuant to §§ 28-1-78 to 28-1-81, inclusive, are confidential. No investigative record may be released except to department personnel, federal, state, and local law enforcement, prosecuting attorneys, and the attorney general in the investigation and prosecution of fraudulent acts. No investigative record or file may be released to any other person except pursuant to a court order. All collection files are confidential. No collection file may be released except in accordance with recipient confidentiality requirements of the department.

CHAPTER 34-20A TREATMENT AND PREVENTION OF ALCOHOL AND DRUG ABUSE
34-20A-90 Records confidential.

34-20A-90. Records confidential. The registration and other records of treatment facilities shall remain confidential and are privileged to the patient.

FEDERAL LAWS, REGULATIONS AND STANDARDS

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Communications Assistance for Law Enforcement Act (1994), 47 U.S.C. § 1001, *et seq.*

Computer Fraud and Abuse Act, 18 U.S.C. §1030

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidential Information Protection and Statistical Efficiency Act of 2002, Pub. L. 107-347, 116 Stat. 2962 44 U.S.C. 3501

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Services (CJIS) Security Addendum CJIS Security Policy, Federal Bureau of Investigation (FBI), CJIS, December 2008, Version 4.5

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Drivers Privacy Protection Act (1994), 18 U.S.C. § 2721

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Electronic Records Electronic Signatures, 21 CFR Part 11, Code of Federal Regulations, Title 21, Part 11

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Information Security Management Act (FISMA) (2002), 44 U.S.C. § 3541(a)(1)(A)

The Privacy Act of 1974, 5 U.S.C. § 552a; 45 C.F.R., Part 5b; OMB Circular No. A-108 (1975)

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Fraud and Related Activity in Connection with Computers, 18 U.S.C § 1030

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

FTC Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501

FTC Standards for Safeguarding Customer Information, Final Rule,16 CFR Part 314

Health Breach Notification Rule (Federal Trade Commission Rule), 16 C.F.R. Part 318

Health Breach Notification Rule (Health and Human Services), 45 C.F.R. Parts 160 and Subparts A and D of Part 164

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

National Security Act, Public Law 235, Section 606, in accordance with Executive Order 13549, **Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities**, August 18, 2010

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Privacy Protection Act (1980), 42 U.S.C. § 2000aa, *et seq.*

Protected Critical Infrastructure Information Program (PCII)

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)

REAL ID Act (2005), H.R. 1268, 109 P.L.13

Right to Financial Privacy Act (1978), 12 U.S.C. § 3401, *et seq.*

Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16 (May 2007)

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

Stored Communications Act, 18 U.S.C. § 2701, et seq.

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272

International Standards

BS 25999 - Business Continuity Management - Part 1: Code of practice

CobiT 4.0 - Level 1

CobiT 4.0 - Level 2

CobiT 4.1

COSO - Enterprise Risk Management - Integrated Framework

ISO 15489 - Part 1

ISO 15489 - Part 2

ISO/IEC 13335 (2004) Part 1

ISO/IEC 17799 (2005) Part 1

ISO/IEC 20000-1

ISO/IEC 20000-2

ISO/IEC 27001 (2005)

AICPA/CICA Generally Accepted Privacy Principles

Indiana Agency Specific Guidance

IOT Policies and Procedures - Information Security Framework

ISP Standard Operating Procedures: Standard Operating Procedure CJD 006 - Department Computers and Systems

ISP Standard Operating Procedures: Standard Operating Procedure CJD 007 - GHQ - Security Access Cards

ISP Standard Operating Procedures: Standard Operating Procedure CJD 008 - Road and Weather Reports - Adverse Weather and Road Conditions

ISP Standard Operating Procedures: Standard Operating Procedure COM 001 - Communications Procedures

ISP Standard Operating Procedures: Standard Operating Procedure COM 010 - Security for Communications Centers, Personnel, and Equipment

ISP Standard Operating Procedures: Standard Operating Procedure INT 002 - Dissemination of Data via IDACS/NCIC

ISP Standard Operating Procedures: Standard Operating Procedure INV 004 - Criminal Intelligence, Crime Analysis, and Criminal Intelligence Report, CIS

ISP Standard Operating Procedures: Standard Operating Procedure PST 001 - Internal Investigations

ISP Standard Operating Procedures: Standard Operating Procedure REC 003 - Reports, Forms, and Record Keeping Procedures

ISP Standard Operating Procedures: Standard Operating Procedure CJD 006 - Department Computers and Systems

ISP Standard Operating Procedures: Standard Operating Procedure COM 001 - Communications Procedures

ISP Standard Operating Procedures: Standard Operating Procedure INT 002 - Dissemination of Data via IDACS/NCIC

ISP Standard Operating Procedures: Standard Operating Procedure INV 004 - Criminal Intelligence, Crime Analysis, and Criminal Intelligence Report, CIS

ISP Standard Operating Procedures: Standard Operating Procedure PST 001 - Internal Investigations

IDACS Standard Operating Procedures - CJIS Systems Agency Information Security Officer – Duties and Responsibilities

IDACS Standard Operating Procedures - Network Configuration Change Management

IDACS Standard Operating Procedures - User Account Creation and Termination

IDACS Standard Operating Procedures -Password Issuance and Management

Indiana Administrative Code Title 240 - Article 5 Communication Systems

Indiana Administrative Code Title 240 - Article 6 Criminal History Record Information

Industry/Organizational Standards and Practices

AGA Report No. 12 - Cryptographic Protection of SCADA

BCI - Good Practice Guidelines 2007

Justice Reference Architecture (JRA) Specification

LEITSC Standards - Law Enforcement CAD Systems

LEITSC Standards - Law Enforcement Records Management Systems

NERC CIP-001-1: Sabotage Reporting

NERC CIP-002-1: Critical Cyber Asset Identification

NERC CIP-003-1: Security Management Controls

NERC CIP-004-1: Personnel & Training

NERC CIP-005-1: Electronic Security Perimeter(s)

NERC CIP-006-1: Physical Security of Critical Cyber Assets

NERC CIP-007-1: Systems Security Management

NERC CIP-008-1: Incident Reporting and Response Planning

NERC CIP-009-1: Recovery Plans for Critical Cyber Assets

NIST Special Publication 800-53

NIST Special Publication 800-53A

NIST Special Publication 800-88: Guidelines for Media Sanitization

PCI DSS v1.2

Appendix B
Glossary of Terms and Definitions

The following is a list of primary terms and definitions that are used throughout this policy or are provided to enhance the reader's understanding of the justice information sharing process.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

Acquiring PLEA— Participating law enforcement agency that uses the Connect South Dakota System to access criminal justice information shared by Originating PLEA(s).

Assimilation—Task of an Originating PLEA in selecting criminal justice information maintained on its records management system to be shared with Acquiring PLEAs on the Connect South Dakota System.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authorized Users—Those persons who have been granted appropriate security access to entity information (for example, a law enforcement official or the prosecuting attorney) when the agency has a "right to know" and the individual has a "need to know" the information for legitimate law enforcement, public protection, public prosecution, or justice purposes and only for the performance of official duties in accordance with law and their agency procedures. Authorized users, for the purposes of the Connect South Dakota System, include Connect South Dakota personnel, Originating and Acquiring PLEA personnel, and authorized Private Contractors providing technical assistance.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term "civil rights" refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon

government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[1]

Computer Security—The protection of information assets through the use of technology, processes, and training.

Confidentiality—Closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Connect South Dakota Project—The project created by the Joint Powers Agreement among PLEAs to operate the Connect South Dakota System.

Connect South Dakota System—The web based computer system that connects individual PLEA information systems to allow for the sharing of information.

Data—Inert symbols, signs, descriptions, measures or elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile entity or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, entity, or organization outside the entity that collected it. Disclosure is an aspect of privacy focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Fair Information Principles—The Fair Information Principles (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Information, Records or Data—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. This may be information that is maintained in a records management system, a CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement entities can be categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

Information Quality (IQ)—Refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of IQ have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, IQ is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment—An approach that facilitates the sharing of terrorism information.

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement entity effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement entities with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or entities.

Law Enforcement Information—Law enforcement information means any information obtained by or of interest to a law enforcement entity or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Logs—A necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Originating PLEA—Participating law enforcement agency that allows criminal justice information maintained in its records management system to be accessed by and shared with Acquiring PLEAs through the Connect South Dakota System.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data—Personal data refers to any information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also PII.

Personally identifiable information—Personally identifiable information (PII) is one or more pieces of information that, when considered alone or in the context of how the information is presented or gathered, can contribute to specify (identify) a unique individual. The pieces of information can be personal data, such as biometric characteristics or a unique set of numbers or characters assigned to a specific individual; behavioral data, such as locations or activities; or, communications such as innermost thoughts and feelings. Information is personally identifiable even if it carries no explicit and immediately apparent indication of the individual to whom it belongs and even if identification of a unique individual is not contemplated at the time the information is collected or in the use to which it is put. For example, personally identifiable information includes pictures of a crowd at a public event, even though no one is yet identified and no one may ever be identified, but it does not include the weather at the event. The fact that the event occurred, if not public information, may also be personally identifiable information since, if put together with an attendance list, it constitutes personally identifiable information about behavior.

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence entity concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement entities, "persons" means United States citizens and lawful permanent residents. [Note—perhaps change this to read: "Persons" means United States citizens and lawful permanent residents.]

PLEA – Participating Law Enforcement Agency is any state or local law enforcement agency that executes the Joint Powers Agreement, including the Division of Criminal Investigation.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the South Dakota Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 12; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by CSD policy or state, local, or tribal law.

Public—Public includes:

- Any natural person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the originating entity or user entity.

Public does not include:

- Employees of the originating entity or user entity.
- People or entities, private or governmental, which assist the entity in the operation of the justice information system.
- Public entities whose authority to access information gathered and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Record—Any item, collection, or grouping of information that includes PII and is maintained, collected, used, or disseminated by or for the collecting entity or organization.

Redress—Laws, policies, and procedures that address public entity responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an entity or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely

availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Shared Information—Criminal justice information an Originating PLEA provides access to and shared with Acquiring PLEAs on the Connect South Dakota System.

Source Agency—Source agency is an entity or organization that has care and custody of a record or document.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.