State of Iowa Department of Corrections

Policy and Procedures

Policy Number: AD-IS-08
Applicability: Institutions, CBC, Central Office, IPI
Policy Code: Public Access
Iowa Code Reference: 904, 904.602
Chapter 1: ADMINISTRATION & MANAGEMENT Sub
Chapter: INFORMATION SYSTEMS/RESEARCH
Related DOC Policies: AD-IS-01, AD-PR-11, AD-PR-29
Administrative Code Reference: 201.5
Subject: IDOC DATA GOVERNANCE
PREA Standards: N/A
Responsibility: Sarah Fineran
Effective Date: October 2024
Authority:

1. PURPOSE

A. The purpose of the current Data Governance Policy is to achieve the following:

1. Establish responsibility for the management of data as an asset.

2. Improve ease of access and ensure that once data is located, users have enough information about the data to interpret them appropriately and consistently.

3. Improve the usage and security of the data, including confidentiality as described in **AD-PR-29** *Confidentiality of Information* and protection from loss.

4. Improve the quality and integrity of the data; resulting in greater accuracy, timeliness, and quality of information for decision-making and reporting.

B. The IDOC Data Governance Policy addresses data governance structure and includes policies on data access, availability, quality, consistency, and security.

2. POLICY

A. Data governance at IDOC was established at the direction of the IDOC Data Governance Council and approved by the Department Director in December 2023.

B. Entities Affected

Anyone using IDOC data who creates, manages, or relies on it for decision making or planning. This includes but is not limited to the following:

1. Central Office
2. Institutional Staff
3. Community Based Corrections
4. Other agencies, institutions, groups, or individuals who collaborate with IDOC or leverage IDOC data

C. Who Should Read this Policy

Data governance executive sponsors, data stewards, and all other employees who use data, regardless of the form of storage or presentation.

3. DEFINITIONS - As used in this document:

A. Data Governance - Purpose is to develop department wide policies and procedures that ensure data meet these criteria within and across IDOC data systems.

B. DOC Governance Council - A body established within the Iowa Department of Corrections to oversee the management, security, and use of data within the department. The Council's primary responsibilities include setting data policies, ensuring compliance with relevant laws and regulations, and promoting best practices for data handling. It serves as the central authority for making decisions related to data governance, including the classification, access, and sharing of data across the department and with external entities.

C. IDOC Data - Assets maintained to support the central missions of reentry, client success, and community safety. Collections of data elements relevant to the operations, planning, or management of any unit at or under the guidance of IDOC, or data that are reported or used in official IDOC reports. To support effective, innovative, and data informed decision making, IDOC data must be accessible, correctly represent the information intended, and must be easily integrated across information systems both within IDOC and externally.

D. Iowa Correctional Offender Network (ICON) - The Iowa DOC's administrative case management system.

CONTENTS

A. Data Governance Structure

B. Data Access & Availability Policy

C. Data Usage and Security Policy

D. Data Quality and Integration Policy

4. PROCEDURES

A. Data Governance Structure

Data Governance is the practice of making strategic and effective decisions regarding IDOC's information assets. It assumes a philosophy of freedom of access to applicable data by all who possess the need, coupled with the responsibility to adhere to all policies and all legal constraints that govern that use. In the interest of attaining effective data governance, IDOC applies formal guidelines to manage information assets and assigns staff to implement them. While the data administrator is assigned a leadership role and oversight for the activities of data governance, this function is shared among the executive sponsors, data stewards, data administrators, and data users. Executive sponsors will appoint data stewards, and through the establishment of data policies and institutional priorities, provide direction to them and data administrators. The data stewards comprise the Data Governance Council, a body that meets regularly to address a variety of data issues and concerns.

1. Overview of Roles for Governing Data

   The following are general descriptions of the primary roles and responsibilities within Data Governance.

   a. Executive Sponsors - Executive Sponsors are senior IDOC staff who have planning and policy responsibility and accountability for major administrative data systems (e.g., Research, Medical, and Fiscal) within their functional areas. By understanding the planning needs,

they are able to anticipate how data will be used to meet those needs. Executive Sponsors may include the following administrative personnel currently in place at IDOC: Research Director, Nursing Director, Security Director, IT Administrator, and Fiscal Officer. Executive Sponsors will meet with the Data Governance Council regularly to address a variety of data issues and concerns.

b. Director of Data Management (Research - DWA) - The Director of Data Management works with the IDOC community to define a statewide structure of data stewardship by making explicit the roles and responsibilities associated with data management and compliance monitoring. This individual is responsible for coordinating data policies and procedures - ensuring representation of the interests of Data Stewards, Managers, and Key Users. The Director of Data Management coordinates the meetings for the executive sponsors and Data Governance Council and provides support to related data management efforts. This individual is also responsible for developing a culture that supports data governance in areas with critical peripheral databases that exist beyond the major administrative systems. The Director of Data Management works to ensure that all IDOC data are represented within a single logical data model that will be the source for all physical data models.

c. Data Stewards - Data Stewards are appointed by executive sponsors to implement established data policies and general administrative data security policies. Data Stewards are responsible for safeguarding data from unauthorized access and abuse through established procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. They support access by providing appropriate documentation and training to support data users. Included among Data Stewards are the following administrative personnel currently in place at IDOC: ICON Master Trainers and Systems Administrators who perform programming or Database Administrator (DBA) roles.

d. Data Administrators - Data Administrators are employees who most often report to Data Stewards and whose duties provide them with an intricate understanding of the data in their area. They work with the Data Stewards to establish procedures for the responsible management of data, including data entry and reporting. Some Data Administrators may work in a technology unit outside of the functional unit, but have responsibilities for implementing the decisions of the unit. Technical Data Administrators may be

responsible for implementing backup and retention plans, or ensuring proper performance of database software and hardware.(Systems Administrators, Information Technology Specialists)

B. Data Access and Availability

1. The purpose of proper data access and availability is to ensure that employees have appropriate access to data and information. While recognizing the department's responsibility for the security of data, the procedures established to protect that data must not interfere unduly with the efficient conduct of business. This policy applies to all units and to all uses of IDOC data, regardless of the offices or format in which the data reside.

2. The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuses, misinterpretation, and unnecessary restrictions to its access. The department will protect its data assets through security measures that assure the proper use of the data when accessed. Data access will be conducted in accordance with the policies established by IDOC and Iowa Code 904. Any employee or non-employee denied access may appeal the denial to the Data Governance Board with their recommendation for decision provided and finalized by the Data Governance Executive Sponsor.

C. Data Usage and Security

1. The purpose of the Data Usage and Security guidance is to ensure that IDOC data are not misused or abused, and are used ethically, according to any applicable law, and with due consideration for individual privacy. Use of data depends on the security levels assigned by the Data Steward.

2. Personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of update, read-only, and external dissemination. Authority to update data shall be granted by the appropriate Data Steward only to personnel whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with the desire to provide excellent service to staff, Executive Leaders, and other constituents.

3. Read-only usage to administrative information will be provided to employees for the support of IDOC business without unnecessary difficulties/restrictions. Only those data elements designated as external can be externally disseminated for official or nonofficial reporting. The release of all other data must be approved by the responsible data steward.

4. Consequence of Noncompliance – Individuals who fail to comply with the data usage guidance, the CJIS Security Policy available through the CJIS Security Policy Resource Center, IDOC Policy **AD-PR-29** *Confidentiality of Information*, and/or **Iowa Code 904.602** may be considered in violation of the IDOC Policy **AD-PR-11** *General Rules of Employee Conduct* and may be subject to disciplinary action or to legal action if laws have been violated. In less serious cases, failure to comply with this policy could result in denial of access to data. Criminal Justice Information Services (CJIS) Security Policy addresses the consequences of a security breach involving criminal justice information. While the policy itself may not explicitly outline every possible consequence, it emphasizes the importance of maintaining the confidentiality, integrity, and availability of criminal justice information and the potential ramifications of failing to do so.

    a. **Reporting Requirements**: Organizations must report any security breaches to appropriate authorities, including the FBI's CJIS Division. This helps ensure that breaches are addressed swiftly and that any potential harm is mitigated.

    b. **Accountability**: The policy stresses that individuals and organizations are responsible for adhering to the security standards set forth. Failure to comply can result in disciplinary action, including potential criminal or civil penalties.

    c. **Access Revocation**: If a breach occurs due to negligence or non-compliance with security protocols, access to CJIS data may be revoked for individuals or organizations involved.

    d. **Impact on Funding and Contracts**: Agencies that do not comply with CJIS security standards may face consequences in terms of funding or eligibility for contracts related to law enforcement and criminal justice.

    e. **Legal Consequences**: Breaches involving sensitive information can lead to legal repercussions, including lawsuits or criminal charges, depending on the nature and severity of the breach.

D. Data Quality and Integration

1. The Data Quality and Integration guidance is to ensure that IDOC data have a high degree of integrity and that key data elements can be integrated across all systems. This is designed so that IDOC staff, stakeholders, and management may rely on data for information and decision support.

2. Data integrity refers to the validity, reliability, and accuracy of data. Data integrity relies on a clear understanding of the business processes underlying the data and the consistent definition of each data element. Data integration, or the ability of data to be assimilated across information systems, is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

3. IDOC data will be consistently interpreted across all systems according to the best practices agreed upon by the Data Governance Council, and it will have documented values in all IDOC systems. Data Administrators will ensure that the needs of users of data are taken into consideration in the development and modification of data structures, domains, and values. It is the responsibility of each Data Steward to ensure the correctness of the data values for the elements within their charge.

4. IDOC data are defined as data that are maintained in support of an IDOC operation and meet one or more of the following criteria:

    a. The data elements are key fields, that is, integration of information requires the data element;

    b. The DOC must ensure the integrity of the data to comply with internal and external administrative reporting requirements, including planning efforts;

    c. The data are reported on or used in official IDOC reports and external requests.

5. It is the responsibility of each Data Steward, in conjunction with the Data Governance Council, to determine which core data elements are part of IDOC data. Documentation, including metadata, on each data element will be maintained within an IDOC repository according to specifications provided by the Director of Data Management and informed by the Data Governance Council. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as timing within our fiscal year calendar. All employees

are expected to bring data problems and suggestions for improvements to the attention of the appropriate data stewards, the Data Governance Council, or the Director of Data Management.