STATE OF IOWA DEPARTMENT OF CORRECTIONS
POLICY AND PROCEDURES

Policy Number: AD-IS-01
Applicability: Institutions, CBC, Central Office & IPI
Policy Code: Public Access
Iowa Code Reference: N/A
Chapter 1: ADMINISTRATION & MANAGEMENT
Sub Chapter: INFORMATION SYSTEMS/RESEARCH
Related DOC Policies: N/A
Administrative Code Reference: N/A
Subject: MANAGEMENT INFORMATION SYSTEMS & DATA SECURITY
PREA Standards: N/A
Responsibility: Sarah Fineran
Effective Date: December 2024
Authority:

1. PURPOSE

To describe the management information systems that will be used in all Iowa Department of Corrections (IDOC) Institutions, Districts, and Central Office (CO).

2. POLICY

It is the policy of the IDOC to maintain a state-of-the-art management information system to assure that IDOC Management has available to them a useful array of well-organized information about Institutional and District operations in order to make informed operational and strategic decisions.

CONTENTS

E. Iowa Corrections Offender Network (ICON) Minimum Data Entry Requirements

F. Reporting

G. Food Service ICON

H. Banking ICON

I. Critical Incident Reporting

J. Medical/Mental Health

K. ICON View

L. Pharmacy

M. PDA

N. KIOSK

O. CBC Fee System

P. Investigations Database

Q. CQI Database

R. Help Desk Ticketing

S. DOC Dashboards

T. Security of Data and Hardware

U. Project Approval Process and Designated Authorities

V. TAC Requirements and Expectations

W. External Dissemination of Data and Requirements

X. External ICON Users and Agencies

Y. Incident Response

3. DEFINITIONS - As used in this document:

A. Criminal Justice Agency (CJA) - A court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

B. Criminal Justice Information (CJI) - All of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

C. Criminal Justice Information Services (CJIS) - Connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.

D. Data Security Team (DST) - A group of professionals within an organization responsible for safeguarding the confidentiality, integrity, and availability of its data assets. Their primary goal is to protect sensitive information from unauthorized access, disclosure, alteration, or destruction. The DST can be reached for inquiry/report through the Help Desk Ticketing System: Assignment Group - DOC - ICON Security.

E. Incident Response Team (IRT) - A group of individuals within an organization tasked with responding to and managing cyber security incidents.

   Reported security incidents to the IRT shall be reported through the ICON Help Desk; Assignment Group - DOC - ICON Security.

F. Local Agency Security Officer (LASO) - A designated person responsible for overseeing the security of CJIS data and systems within a local agency.

G. Master Control Agreement (MCA) - A document which stipulates management control of the criminal justice function remains solely with the CJA.

H. Non-Criminal Justice Agencies (NCJA) - (for the purposes of access to CJI) As an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

I. Personally Identifiable Information (PII) - Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying

information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

J. Personal Digital Assistant (PDA) - A handheld device designated to assist individuals with various organizational functions.

K. Terminal Agency Coordinator (TAC) - The point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

4. PROCEDURES

A. Guidelines

1. Each IDOC Institution, District, and Central Office will use an organized system of information collections, storage, retrieval, reporting, and review, to be integrated with the institution's short and long range planning processes.

2. The system will be under the supervision of the Research Director, to assure a continuous evaluation of the IDOC and individual institutions/districts.

3. The information generated will be used to facilitate reviews of specific programs and assess immediate goal achievement against established criteria.

4. The system will be capable of identifying trends in population movement, referral and intake systems.

5. The system will be capable of delivering demand information when special reports are required.

B. Operation of the System

1. The information collection system will be directly related to the IDOC's goals, objectives, and performance measures will be comprised of data sets identified as useful for management purposes.

2. The IDOC will maintain primary responsibility for operation of information systems in the areas of personnel, procurement, and general finance.

3. The Warden, District Director, and CO will assign staff to operate the automated information system being sure they are properly trained with security and confidentiality needs being addressed.

C. System Capabilities

The Central Office staff will determine the systems capability for gathering, organizing, and reporting information by performing the following tasks on at least an annual basis:

1. Reviewing each Institutions, Districts and CO goals and objectives to be sure data being supplied measures the level of achievement desired.

2. Providing written summaries of findings to ensure potential demand information is provided by the management information system.

D. Data Content

1. Certain standard information along with local Institutions, Districts, and Central Office needs will be part of the system.

2. The kinds of information collected will include the following:

   a. Institutions and Districts maintain a single master index identifying all incarcerated individuals assigned to the Institution or District.

   b. General incarcerated individual/client characteristics

   c. Program activities and completions

   d. Incidents in Institutions and Districts.

   e. Significant intake information arrests (only as the result of supervision, presentence investigation or prison), age, cultural background, type of offense)

E. Iowa Corrections Offender Network (ICON) Minimum Data Entry Requirements - See Business Rules in ICON for the minimum data required to be entered in ICON for institutions and districts. This document can be found under the HELP button of all 3 Intake screens: Field-Intake Data Collection, Institution-Intake Data Collection, and Residential-Intake Data Collection or under System > Help > Business Rule Documents, click the General Help File checkbox, then click search.

F. Reporting

The system will generate management and line staff reports from a variety of software and hardware platforms.

G. Food Service ICON

1. Inventory

2. Operations

3. Meal Tracking

H. Banking ICON

1. Primary Accounts

2. Obligations

3. Revenues

4. Expenditures

5. Commissary

6. Lock Box

7. Debit Cards

I. Critical Incident Reporting

All Priority One and Two Critical Incidents will be entered in accordance with **AD-GA-06** *Critical Incident Reporting*.

J. Medical/Mental Health

1. Multi-level Scheduling System

2. Medical Records

3. Physician Orders

4. Workload Management

K. ICON View

1. Financial Transactions
2. Phone calls
3. Email Messages
4. Visits

L. Pharmacy
1. Drug Utilization Review
2. Patient Profile Information
3. Formulary/Non-Formulary Order Checks
4. Inventory Management

M. PDA
1. Counts
2. Rounds
3. Security Standards
4. Generic Notes

N. KIOSK (Institution and District)
1. Public Messaging
2. Contact List
3. Commissary
4. Banking Information - funds management for phone and o'mail
5. Staff Messaging
6. Contact Phone Management
7. Prescription Refill Request

8. Law Library

9. O'mail - Inbound/Outbound o'mails from approved addresses

10. Bulletin Board

11. Policy Documents

O. CBC Fee System

P. Investigations Database

Q. CQI Database

R. Help Desk Ticketing

S. DOC Dashboards

1. ICON Dashboard

2. SAS Dashboards

3. Enterprise Data Warehouse

T. Security of Data and Hardware

1. Data needs to be safeguarded to prevent theft or unauthorized use

2. The information that this system entails may be shared with, and may contain data provided by, other agencies and organizations in the criminal justice system.

3. To the degree practical and within applicable state laws regulations, data systems will be standardized to facilitate data interchange.

U. Project Approval Process and Designated Authorities

1. ICON programming requests and ICON related projects must be initiated using the IDOC Help Desk Ticketing.

2. Approval of ICON system programming requests and ICON related projects must be vetted by the Department's Research Coordinator.

3. Purchasing decisions relating to ICON programming and ICON related projects will be made and authorized by the Department's Research Coordinator in collaboration with the Department's Fiscal Officer.

V. TAC Requirements and Expectations

1. Each prison and district are expected to have an appointed Terminal Agency Coordinator (TAC) at all times. The TAC for CJIS Security Awareness plays a crucial role in ensuring that the organization maintains the highest standards of security when handling sensitive criminal justice information.

2. TAC Assignments must be reported to the Research Team. Prisons and Districts must appoint a replacement TAC within 30 days of TAC's departure. A list of TACs are maintained by the Data Governance Board.

3. TACs are responsible for ensuring all staff newly hired or appointed receive CJIS Security Awareness Training prior to provision of ICON. (Note: IDOC interns shall have ICON permissions granted to them based on the job duties of the internship and placed into the appropriate statewide ICON Security Groups.)

4. TACs are responsible for ensuring all staff complete CJIS Security Awareness Training annually.

5. TACs are responsible for:

   a) Training and Coordination: Organizing and coordinating training sessions on CJIS security policies, procedures, and best practices for employees who handle criminal justice information.

   b) Policy Enforcement: Ensuring that all employees adhere to CJIS security policies and procedures in their daily activities. This involves monitoring compliance, addressing any violations, and implementing corrective actions as necessary.

c) Incident Response: Developing and implementing procedures for responding to security incidents or breaches involving criminal justice information. This includes investigating incidents, containing the impact, and reporting to appropriate authorities as required by CJIS security policies.

d) Security Awareness Campaigns: Developing and promoting security awareness campaigns to educate employees about the importance of CJIS security and their role in maintaining it.

e) Documentation and Reporting: Maintaining detailed documentation of security procedures, training records, incident reports, and other relevant information. Documentation is essential for demonstrating compliance with CJIS security requirements and may be subject to audits by law enforcement agencies.

f) Coordination with CJIS Compliance Auditors: Serving as the primary point of contact for CJIS compliance auditors and assisting with audits of the organization's security practices. This involves providing access to relevant documentation, facilitating interviews with staff, and addressing any findings or recommendations from the audit.

g) Continuous Improvement: Proactively seeking opportunities to enhance the organization's CJIS security posture through process improvements, technology upgrades, and employee training initiatives. This may involve staying updated on emerging security threats and industry best practices.

W. External Dissemination of Data and Requirements

1. All external requests for data and/or any type of data exchange must be processed through the Research team.

2. Provision of case-level data for an external entity is contingent on signing a Management Control Agreement (MCA).

   MCA’s will be issued by the Research Division in accordance with the Security Team’s review for approval of third party ICON access.

X. External ICON Users and Agencies

1. The IDOC understands that entities outside the IDOC may have a need for ICON access.

2. External agencies must appoint a TAC to act as the point of contact for agency ICON access requests and verify CJIS training requirements are met.

3. External requests for access are to be made to the Research team who will triage the request with the Department's Data Security Team (DST). External requests for access will be documented in HelpDesk ticketing.

4. External users requesting ICON access must submit a Personnel Action ICON Access Request form:

   a) Have no record of current or former correctional supervision.

   b) List all family members, which includes immediate and extended, with current or former correctional supervision. Failure to accurately or truthfully disclose this information may result in non-access.

5. All Non-Criminal Justice Agencies with external ICON end users must sign a MCA.

6. Criminal Justice Agencies with external ICON end users must sign a Memorandum of Understanding.

Y. Incident Response Incident Data Leakage

1. Incident Data Leakage

   a) This incident response procedure is integrated with the broader data leakage prevention policy and procedures of the Iowa Department of Corrections. Regular testing and rehearsal of the incident response plan through tabletop exercises or simulated incidents can help ensure its effectiveness in real-world scenarios.

   b) Detection

      1) Internal Monitoring: Regular monitoring and auditing of data access logs, network traffic, and system activities shall be conducted to detect any anomalies or suspicious behavior indicative of data leakage.

2) Employee Reporting: All personnel who suspect or become aware of a potential data leakage incident must immediately report it to their supervisor or designated authority.

c) Incident response for NCIC system outage issues

Contact DPS at PSB-ACT@dps.state.ia.us; (515) 725-6220 or (800) 363-2297

d) Incident response for NCIC vendor: OpenFox

1) A ticket can be sent to support@openfox.com; (630) 854-8112

2) This address can be used for OpenFox NCIC inquiries which will not generate a ticket: supportcenter@openfox.com

2. Preliminary Assessment

a) Upon receiving a report or detecting a potential incident, the DST shall conduct a preliminary assessment to determine the nature and scope of the incident.

b) The DST shall gather relevant information, including the time and location of the incident, the type of data involved, and any potential impact on departmental operations or individuals' privacy.

3. Containment and Mitigation

a) Immediate steps shall be taken to contain the incident and prevent further unauthorized access or dissemination of sensitive data.

b) The Incident Response Team (IRT) shall isolate affected systems or networks, disable compromised accounts, and implement additional security controls as necessary to mitigate the risk of further data leakage.

4. Investigation

a) A thorough investigation shall be conducted to determine the cause of the data leakage incident, identify the source of unauthorized access or disclosure, and assess the extent of the damage.

b) The investigation may involve forensic analysis of digital evidence, interviews with relevant personnel, and collaboration with internal or external security experts.

5. Notification

    a) If the data leakage incident involves Personally Identifiable Information (PII) or other sensitive data subject to legal or regulatory requirements, affected individuals, regulatory authorities, and other relevant stakeholders shall be promptly notified in accordance with applicable laws and regulations.

    b) Notifications shall include a description of the incident, the type of data compromised, and any remedial actions taken or recommended.

    c) If the data leakage involves Criminal Justice Information (CJI) contact the Security Operation Center (SOC) at (855) 442-4357 or (515) 725-1296.

6. Remediation

    a) Once the investigation is complete, remedial actions shall be taken to address any vulnerabilities or deficiencies identified during the incident response process.

    b) This may include implementing additional security controls, updating policies and procedures, providing additional training to personnel, or making changes to systems or infrastructure.

7. Documentation

    a) Detailed documentation of the incident response process, including all actions taken, findings, and outcomes, shall be maintained for future reference and analysis. Documentation will be retained by the Research Director.

    b) Incident reports shall be submitted to the appropriate authorities, including regulatory agencies, legal counsel, and senior management, as required.

8. Review and Lessons Learned

    a) After the incident has been resolved, a post-incident review shall be conducted to assess the effectiveness of the response process and identify any lessons learned.

    b) Recommendations for improvements to policies, procedures, or security controls shall be documented and implemented to strengthen the department's overall security posture.

9. Follow-up

    a) Ongoing monitoring and follow-up activities shall be conducted to ensure that the incident response process remains effective and that any identified vulnerabilities are addressed promptly.

    b) Regular training and awareness programs shall be conducted to educate personnel about data leakage risks and prevention measures.

10. Reporting

    A final incident report shall be prepared summarizing the incident, response activities, and lessons learned, and submitted to senior management and relevant stakeholders for review and approval.