State of Indiana Indiana Department of Correction	Effective Date	Page 1 of	Number
	12/1/2020	8	04-05-107

POLICY AND ADMINISTRATIVE PROCEDURE
Manual of Policies and Procedures

Title
SENSITIVE DATA CATEGORIZATION REQUIREMENTS

Legal References (includes but is not limited to)	Related Policies/Procedures (includes but is not limited to)	Other References (includes but is not limited to)
11-8-5-2	04-03-101 04-03-103 04-03-111	IOT-CS-SEC-102 NIST 800-53 Rev 4

I. PURPOSE:

The purpose of this policy is to define the process for identifying, classifying and labeling Indiana Department of Correction (IDOC) data pursuant to the requirements of the Indiana Office of Technology, Data Categorization, which is derived from NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

II. POLICY STATEMENT:

It is the policy of the Indiana Department of Correction to identify, classify and label data on an annual basis pursuant to the requirements of Indiana Office of Technology, Data Categorization, which is derived from NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. This policy and the following administrative procedure shall govern the collection, storage, access, use, and transmission of sensitive or confidential data. This policy and administrative procedure shall be reviewed annually and updated as necessary.

III. DEFINITIONS:

For the purpose of this policy and administrative procedure, the following definitions are presented:

A. AUTHORIZED USER: An IDOC employee, contractor, intern, volunteer or other agent of the State who is authorized at a technical level to administer and support/maintain state computing information technology systems or is authorized at an end user level, to have access to and use State computing information technology systems and telecommunications technology systems for business purposes on behalf of the State of Indiana.

B. AVAILABILITY: Ensuring timely and reliable access to and use of data/information.

C. CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including the means for protecting privacy and proprietary information.

D. DATA: For the purposes of this policy and administrative procedure, the coded representation of quantities, objects, and actions. The term "data" is often used interchangeably with the word "information" in common usage and in this policy and administrative procedure.

E. DATA CLASSIFICATION LABELS: The level of protection based on the confidentiality and criticality requirements of data in accordance with the Department's risk assessment. Data classification labels enable policy-based standards for securing and handling data and sharing among organizations. The terms, "data classification label," and "classification label," are used interchangeably in this policy.

F. DATA CUSTODIAN: IDOC authorized users at the technical level responsible for the safe custody, transport, and storage of State data as well as the implementation of any applicable federal, State, or Department data protection requirements.

G. DATA OWNERS: IDOC managing directors or designees that are authorized users responsible for identifying and classifying data for their respective areas.

H. INFORMATION: For the purposes of this policy and administrative procedure, data processed into a form that has meaning and value to the recipient to support an action or decision. The term "information" is often used interchangeably with "data" in common usage and in this policy and administrative procedure.

I. INFORMATION SECURITY OFFICER (ISO): The technical staff member of IDOC that, in collaboration with the Indiana Office of Technology, Executive Director of Technology Services, and other IDOC technical staff members, is responsible for the security oversight of IDOC's information technology system assets by establishing appropriate system asset security standards and risk controls to identify, develop, implement, maintain, and support security processes across the IDOC information technology resources and to respond to system asset security incidents.

J. MEMORANDUM OF UNDERSTANDING (MOU): A written document describing a bilateral or multilateral agreement between two (2) or more parties. An approved MOU executed by all parties is required before any non-IDOC party receives IDOC data in an electronic or paper form. At a minimum, the MOU shall contain references pertaining to IDOC and the Indiana Department of Administration, Office of Information Technology (IDOA IOT)

data security policies, standards, bulletins, directives, and guidelines that the non-IDOC party must follow in order to receive IDOC data.

K. INTEGRITY: For the purposes of this policy and administrative procedure, guarding against improper information modification or destruction, and includes ensuring data/information non-repudiation and authenticity.

L. PERSONALLY IDENFIABLE INFORMATION (PII): Information that can be used directly or in combination with other information to identify a particular individual. PII includes a name, identifying number, symbol, or other identifier assigned to a person; any information that describes anything about a person; any information that indicates actions done by or to a person, and any information that indicates that a person possesses certain personal characteristics.

M. SENSITIVE DATA: Sensitive data is any type of data that presents a high or medium degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a medium risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. The data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

IV. PROCEDURES:

A. IDOC information systems shall be identified, classified, and labeled by availability and confidentiality:

1. Availability identifies the degree of need for data to maintain its integrity and accessible. IDOC data shall be assigned one of three labels for availability:

a. Critical: The loss of data integrity or availability would result in severe or catastrophic adverse effect. A severe or catastrophic adverse effect means that, for example, the loss of integrity or availability might cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary function; result in major damage to organizational assets; result in major financial loss or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

b. Necessary: The loss of data integrity or availability would result in a serious adverse effect. A serious adverse effect means that, for example, the loss of integrity or availability might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to organizational assets; result in significant financial loss or result in significant harm to individuals, that does not involve loss of life or serious life threatening injuries.

c. Non-critical: The loss of data integrity or availability would result in limited adverse effect. A limited adverse effect means that, for example, the loss of integrity or availability might cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; result in minor damage to organizational assets; result in minor financial loss or result in minor harm to individuals, including privacy.

2. Confidentiality identifies how sensitive the data is with regard to unauthorized disclosure and the resulting adverse effects of the unauthorized disclosure. Adverse effects on individuals may include, but are not limited to, the loss of privacy. IDOC data shall be assigned one of three confidentiality labels:

a. Confidential: This classification includes information that is the most sensitive for use within the State or Department only. The classification of information is exempt from disclosure under the provisions of the Freedom of Information Act, HIPAA, or other applicable federal laws or regulations. Its unauthorized disclosure could seriously or adversely impact the State, Department, its business partners, customers, or individual persons. Examples include but are not limited to: Health care, law enforcement, taxpayer information, and personal financial information.

b. Sensitive: This classification includes information requiring special precautions to assure the integrity of the information and protection from unauthorized modification or deletion. This classification of information require a higher than normal assurance of accuracy and completeness. Examples of sensitive information include but are not limited to: financial transactions and regulatory actions.

c. Private: This classification includes personal information that is intended for use within the State or Department. Unauthorized disclosure could seriously or adversely impact the State or Department and/or its employees.

d. Public: This classification includes information not clearly fitting into any of the above three classifications. Disclosure may be limited in some cases by policy. Disclosure

does not negatively impact the State, agency, its employees and/or customers. Public information is categorized as follows:

1) Public Controlled: Information is public but accuracy must be maintained and access must be controlled by specific procedures (e.g., DMV records); and,

2) Public Published: Accuracy is not as critical and the information is freely published or posted (e.g., telephone directory).

B. The following IDOC authorized users shall be responsible for data identification and classification:

1. IDOC Data Owners shall:

a. Follow the data requirements specified in Indiana Office of Technology and IDOC policies, standards, and guidelines pertaining to information access, use, security, and protection.

b. Assign data classifications based on IDOC's business requirements and risk assessment results provided by the ISO.

c. Ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data. Summary data drawn from various information sources may be classified at a lower level of confidentiality than the original information so long as the individual data from which the summary is derived is not apparent or not revealed.

d. Ensure that the data shared between IDOC and another agency is consistently classified and protected in accordance with a written memorandum of understanding (MOU), which, at a minimum, shall contain the following statements pertaining to ODRC and DAS OIT's data security requirements:

"*In order to ensure the security of IDOC data, the (name of non-IDOC party receiving IDOC data) hereby agrees to fully comply with all IDOC and Indiana Office of Technology data security policies, standards, bulletins, directives and guidelines. Said IDOC and IOT policies, standards, bulletins, directives and guidelines are available for review by request from IDOC or IOT.*"

e. In consultation with ISO, ensure that sensitive data or PII is secured in accordance with applicable agency requirements, and federal or State regulations and guidelines.

f. Develop, in consultation with the ISO, data access qualification guidelines for each data classification label in their operational area, keeping in mind that more secure levels of data classification shall require more stringent access qualifications. Data access qualification guidelines shall be required for all authorized users.

2. IDOC Data Custodians shall:

   a. Follow the requirements specified in IDOC and IOT data security policies, standards, bulletins, directives, and guidelines pertaining to information access, use, security, and protection, which shall include ensuring the appropriate written MOU containing all the necessary data security requirements mandated by IDOC and has been completed and fully executed by IDOC and the non-IDOC party requesting IDOC data before sharing any IDOC data with the non-IDOC party.

   b. In consultation with the ISO, ensure that proper access controls are implemented and that the controls are monitored and audited for IDOC facility, floor and/or cage access in accordance with the data classification labels assigned by the data owner.

   c. In consultation with the ISO, complete data audits and security assessments and submit an annual report to the data owners which addresses data security, data availability, data processing integrity and data confidentiality and privacy.

   d. Periodically validate data integrity.

3. IDOC authorized users at an end user level shall ensure that the appropriate written MOU containing all the data security requirements mandated by IDOC has been completed and fully executed by IDOC and the non-IDOC party requesting IDOC data, follow the data requirements specified in IDOC and IOT security policies, standards, bulletins, directives, and guidelines pertaining to information access, use, security and protection, and understand that particular types of data, such as PII and sensitive data, may have specific access and use limitations.

C. IDOC shall use the following process to identify, classify, and label data:

1. On an annual basis, in consultation with the ISO or designee, IDOC data owners or their administrative designees shall identify the data and data systems in their operational areas, including data and data systems compiled from multiple sources, data shared between IDOC and other agencies, sensitive data, and PII and shall:

a. Identify any regulatory changes, such as new statutes or rules that have been implemented in the last year that impact access, use or management of the data under their control'

b. Identify any technology changes, such as the distribution of new mobile computing devices that have occurred in the last year that impact access, use or management of the data under their control;

c. Assess their data and data systems and assign data classification labels to the data and data systems, pursuant to the requirements of this policy. Summary data drawn from multiple sources may be classified at a lower level of confidentiality than the original information so long as the individual data from which the summary is derived is not apparent or not revealed;

d. Verify that a documented, formal agreement that contains data treatment requirements, such as a MOU, exists between IDOC and other agencies for any of the data under their control shared with other agencies;

e. Verify that their sensitive data or PII is secured in accordance with applicable agency requirements, and federal or state regulations and guidelines;

f. Verify that data access qualification guidelines exist for each data classification label in their operational area; and,

g. Document the above noted process in a formal manner.

2. On an annual basis, the ISO or designee shall complete a compliance review of each data owner's efforts to comply with the processes mandated in this policy and administrative procedure. During the compliance review, the ISO or designee shall meet with each data owner or administrative designees and collect and compile all documentation maintained by the data owner that supports their efforts to comply with this policy and administrative procedure.

3. When all annual compliance reviews are completed, the ISO or designee shall use the information generated during the compliance review to complete an IDOC compliance review report that contains the findings of each data owner's compliance efforts and associated action plans or remediation recommendations to improve compliance. The report shall be submitted to the Executive Director of Technology Services.

IV. APPLICABILITY:

This policy and administrative procedure is applicable to all Department facilities, staff, and offenders, except those offenders on Parole, and to those facilities that are operating under a court order or consent decree that mandates different procedures.

signature on file
Robert E. Carter, Jr.
Commissioner

Date