NORTH Dakota | Information Technology
Be Legendary.

Created: 10/19/2022
Revised: 05/16/2023
Reviewed: 05/16/2023

State of North Dakota Data Classification Policy

Contents

INTRODUCTION **1**

1.0 PURPOSE *1*

2.0 SCOPE *1*

3.0 STATEMENT OF MANAGEMENT COMMITMENT *1*

4.0 DEFINITIONS *1*

PART 1. DATA CLASSIFICATION POLICY **2**

DATA CLASSES *2*

DATA CLASSIFICATION AND REVIEW REQUIREMENTS *2*

PART 2. DATA CLASSIFICATION ROLES AND RESPONSIBILITIES **3**

PART 3. DATA TYPE CLASSIFICATIONS **5**

PART 4. SAFEGUARDING DATA **9**

CHANGES TO DATA *9*

DATA CONTROLS *9*

APPENDIX. SUPPLEMENTAL GUIDANCE **10**

DATA CONTROLS REFERENCE *10*

DATA TYPES REFERENCE *11*

REVISION HISTORY *12*

INTRODUCTION

1.0 PURPOSE

The purpose of the Data Classification Policy is to ensure that data is classified and handled consistently and securely, and that all employees understand their roles and responsibilities with respect to data protection. The policy specifies the categories and criteria for classifying data and a reference model of the protection controls for each category.

2.0 SCOPE

This policy applies to all data and to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e., campuses and agricultural and research centers.

3.0 STATEMENT OF MANAGEMENT COMMITMENT

The North Dakota Chief Information Officer (CIO) directs that Information Technology (IT) Policy be created, as defined within the North Dakota Century Code (Chapter 54-59-09). The Governance Review Team is responsible for review and updating of this policy. Reviews and updates to the policy and procedures will be a coordinated effort, and be routinely reviewed and updated annually, or as immediate changes are required.

North Dakota's Chief Information Security Officer (CISO) directs that this security and privacy policy is created to provide appropriate security and privacy safeguards and countermeasures against the threats and vulnerabilities that may impact the confidentiality, integrity, and/or availability of information and information systems managed by NDIT.

4.0 DEFINITIONS

Controls – Measures put in place to protect data from unauthorized access, modification, or destruction. These controls can take many forms, including technical measures such as encryption and access controls, as well as administrative processes such as data classification and user training.

Data – Any form of information, including paper documents and digital data stored on any type of media.

Data Classification – The assignment of defined labels to data based on shared characteristics or attributes.

Data Type – A named set of data, such as personally identifiable information (PII), protected health information (PHI), or financial transaction information (FTI).

PART 1. DATA CLASSIFICATION POLICY

Data classification establishes a common labeling model based on potential risk. The risk level is determined by assessing the impact on the state or its citizens from the unauthorized access, modification, or destruction of data.

DATA CLASSES

All data must be classified into one of three classes: 1) Low Risk, 2) Moderate Risk, or 3) High Risk. Data not explicitly classified as High Risk or Low Risk shall be classified as Moderate Risk data. The following table summarizes the three data classes:

Data Classifications		
Low Risk	**Moderate Risk**	**High Risk**
1. The data is intended for public disclosure. 2. Unauthorized disclosure, alteration, or destruction of the data would result in little or no risk to the state and its citizens.	1. The data is not generally available to the public. 2. Unauthorized disclosure, alteration, or destruction of the data could result in a moderate level of risk to the state or its citizens.	1. The data requires protection by law/regulation. 2. Unauthorized disclosure, alteration, or destruction of the data could cause a significant level of risk to the state or its citizens.

Table 1 Data Classification Summary

DATA CLASSIFICATION AND REVIEW REQUIREMENTS

All data under the stewardship or ownership of the state must be classified. The data steward will conduct data classification reviews at least annually, or whenever a change occurs that may affect the risk classification of the data.

PART 2. DATA CLASSIFICATION ROLES AND RESPONSIBILITIES

The following roles and responsibilities are established for carrying out this policy:

I. Data Owner – The Data owner is the executive decision maker on data policy and usages in their domain. They are accountable for the overall management and handling of their domain data.

The data owner shall address the following:

- Data classification policy and management oversight – Serve as executive owner of their domain's data policy and provide approval authority for exceptions to policy
- Assign data steward role(s) – Assign individuals to data steward roles
- Data sharing coordination – Facilitate agreements for data sharing between parties

II. Data Steward – Data stewards are individuals with assigned or delegated responsibility for the direct operational-level management of data.

The data stewards shall address the following:

- Data classification – Assign and periodically review data classification labels
- Data compilation – Ensure that data compiled from multiple sources is classified with the highest risk level of any individually classified data
- Data access (in conjunction with data custodians) – Develop data access guidelines for each data classification label
- Data classification compliance (in conjunction with data custodians) — Ensure that data categorized as moderate and high risk is secured in accordance with state and federal laws
- Data policy implementation – Manage the implementation of data policies
- Data sharing – Review, approve, and monitor data sharing requests

III. Data Custodian – Data custodians are responsible for the aggregation, storage, and management of data sets. Their focus is on the "how" rather than the "why" of data storage and management.

The data custodian is responsible for, but not limited to, addressing the following:

- Data classification compliance (in conjunction with data stewards) – Fulfill the data requirements specified by security policies and standards pertaining to information security and data protection. Ensure that data is secured in accordance with state and federal laws
- Implementation of controls – Responsible for operationalizing the controls required by the classification. Possible controls include Access, Audit, Backup and Restoration, Retention, Secure Storage, Validation, etc...

IV. Data User – Data users are individuals who create, need, or use data as part of their assigned duties or in fulfillment of assigned roles or functions. Individuals who are given access to moderate and high-risk data are responsible for protecting the security and integrity of the data. Data users must use data in a manner consistent with the purpose intended and comply with this policy and all policies applicable to data use.

PART 3. DATA TYPE CLASSIFICATIONS

Low Risk – The following types of data are classified as Low Risk (not a complete list):

I. Prepared Open Record Data – Data that has been prepared to fulfil an open records request. This data is open to public inspection according to state and federal law.

II. Publicly Available Data – Data that is readily available to the general public through public sources.

Moderate Risk – The following types of data must be classified, at a minimum, as Moderate Risk and is subject to legislative changes (not a complete list):

I. Operational Data – Data used to support the day-to-day operations of the organization. This includes data such as: employee records, customer information, financial transactions, and other types of data that are essential to the organization's function. Operational data is typically considered to be of moderate sensitivity, as it is not highly confidential but is still important to the organization and needs to be protected from unauthorized access or tampering. As such, operational data typically requires a reasonable level of controls to protect its confidentiality and integrity.

II. Personally Identifiable Information (PII) – PII is data that can be used to distinguish or trace an individual's identity. PII does not include publicly available information that is lawfully made available to the public from federal, state, or local government records. Some individual PII elements or combination of elements must be classified as High Risk PII.

III. Public Employee Personnel Information – Data maintained by state entities that includes, but is not limited to, the information defined in NDCC 44-04-18.1.

IV. Trade Secrets – Trade secrets per NDCC 47-25.1-01(4) is information, including a formula, pattern, compilation, program, device, method, technique, or process, 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.

High Risk – The following types of data must be classified as High Risk. This is not a complete list and is subject to legislative changes.

I. Criminal Justice Information (CJI) – CJI applies to confidential Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (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 and incident history data.

II. Computer Password and Security Information – Per NDCC 44-04-27, this includes security codes, passwords, combinations, or security-related plans used to protect electronic information or to prevent access to computers, computer systems, or computer or telecommunications networks of a public entity.

III. Federal Aviation Administration (FAA) Data – Data that is collected, processed, or used by the FAA in carrying out its regulatory functions. This could include information about aircraft, pilots, airports, air traffic, and other aspects of the aviation industry. The handling of FAA data must comply with Federal Information Processing Standards (FIPS) controls.

IV. Federal Tax Information (FTI) – FTI is any return or return information received from the Internal Revenue Service (IRS) or secondary source, such as from the Social Security Administration (SSA), Federal Office of Child Support Enforcement, or the Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information. The handling of FTI data must comply with Federal Information Processing Standards (FIPS) controls.

V. Financial Information – Governed by Gramm-Leach-Bliley Act (GLBA), this information includes bank account number, routing number, account balance, debt status, or credit score.

VI. High Risk PII – High Risk PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are high risk as stand-alone data elements, and this includes:

1) Social security number (SSN) - full or truncated to last four digits
2) Driver's license or state identification number
3) Passport number
4) Financial account number

Some PII data elements, when combined with other data, must be categorized as high risk. Such combinations include, but are not limited to, those defined in NDCC 51-30-01(4), which includes combinations of an individual's first name or first initial and last name with any of the following data elements when the name and any of the following data elements are not encrypted:

1) The individual's social security number
2) The operator's license number assigned to an individual by the department of transportation
3) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts
4) The individual's date of birth
5) The maiden name of the individual's mother
6) Medical information, including individual's medical history, mental or physical condition, or medical treatment of diagnosis by a health care professional.
7) Health insurance information, including health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual
8) An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password
9) The individual's digitized or other electronic signature

VII. Payment Card Industry (PCI) Data Security Standard (DSS) – Applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personal identification numbers, passwords, and card expiration dates.

VIII. Protected Health Information (PHI) – Governed by Health Insurance Portability and Accountability Act (HIPAA) of 1996 and state laws that address the storage of confidential state and federal personally identifiable health information that is protected from disclosure. PHI is confidential health care information related to an individual's past, present, or future health conditions, including behavioral health information.

IX. Security Vulnerability and Risk Assessment – Disaster and Cybersecurity Information – Per NDCC 44-04-24, this includes any data relating directly to the physical or electronic security of a public facility or critical infrastructure, as well as information relating to cybersecurity defenses or threats, assessments, response plans, and emergency evacuation plans.

X. Social Security Administration (SSA) – Information that is obtained from the Social Security Administration. This can include a Social Security number verification indicator or other PII data.

XI. Student Records PII – Federal Educational Rights and Privacy Act (FERPA) generally prohibits the improper disclosure of personally identifiable information derived from education records.

The following table summarizes the classification of common data types:

	Low Risk	Moderate Risk	High Risk
Data Types	• Prepared Open Record Data • Publicly Available Data	• Operational Data • PII • Public Employee Personnel Information • Trade Secrets	• CJI • Computer Password and Security Information • FTI • Financial Information • High Risk PII • PCI-DSS • PHI / HIPAA • Security Vulnerabilities and Risk Assessments • SSA • State Tax Information • Student PII / FERPA

Table 2 Data Type Classification Examples

PART 4. SAFEGUARDING DATA

CHANGES TO DATA

Significant changes to data, such as, but not limited to, aggregation, commingling, or decoupling, can affect the risk classification of the data.

Any time data is joined, blended, merged, summarized, or analyzed, the classification of the resulting dataset or output must be reviewed. If data is merged/blended, the data needs to be classified at the highest classification of any individual data element. When data is summarized through analysis (such as a presentation of summary counts, mean, median, range, standard deviation, etc., across all fields or by category), the summary data may, in some cases, be classified at a lower-risk classification.

Aggregation is the blending or merging of separate datasets into a single data source. If data with different classifications is aggregated, the highest classification must be applied to all the compiled data.

Commingling is when data of different classifications reside on the same storage medium. All attempts must be made to ensure that there is controlled separation of different data types within the same storage medium. When deemed impossible, the data must be classified to the highest classification level with the most stringent security controls implemented.

Decoupling is the separation or dissociation of data (e.g., into multiple data sources or data sets). If data is decoupled, the appropriate classification must be applied to each separate data set. In some situations, data may be decoupled to remove high risk data elements, so that lower risk data elements may be used or shared.

DATA CONTROLS

Data controls are measures put in place to protect data from unauthorized access, modification, or destruction. These controls can take many forms, including technical measures such as encryption and access controls, as well as administrative processes such as data classification and user training. The specific data controls implemented will vary depending on the classification of the data being protected, as well as the risks and threats facing the organization. The goal of data controls is to ensure the confidentiality, integrity, and availability of data, while also meeting regulatory and compliance requirements.

APPENDIX. SUPPLEMENTAL GUIDANCE

DATA CONTROLS REFERENCE

The following table is not a comprehensive list of all possible data controls. It is intended to illustrate potential controls based on risk classification. In practice, data controls will be specified by the assigned data steward, in consultation with Security Governance, Risk and Compliance (GRC) team, to the specific needs of the agency and align with the enterprise and agency specific policies.

Activity / Classification	**Low Risk**	**Moderate Risk**	**High Risk**
Data Access and Handling Controls			
User Access – Authentication	No authentication needed	Must use NDGOV accounts only	Must use NDGOV accounts with Multi-Factor Authentication (MFA)
Access Audit	n/a	Role-based	Required
End User Training	n/a	Role-based	Required
Data Sharing	n/a	Require data steward approval	Restricted; Require data steward approval
Data Transmission and Communication Controls			
Sent in Email	n/a	Include a disclaimer	Must be encrypted, consider secure alternative
Internal Network Transmission	n/a	Consider encryption	Must be encrypted
External Network Transmission	n/a	Consider encryption	Must be encrypted
Access from External Network	n/a	Must use VPN	Must use MFA VPN
Spoken/Verbal Communication	n/a	Consider confidential use of landlines or secure communication apps	Require confidential use of landlines or secure communication apps
Fax	n/a	Consider encryption	Encrypt, consider secure alternative
Data Storage and Media Controls			

Activity / Classification	Low Risk	Moderate Risk	High Risk
Stored on the Local Network or Cloud	n/a	Authentication required, consider encryption	Authentication required, must be encrypted
Stored on Portable Electronic Devices – Smart Phones and Tablets	n/a	Authentication required, must have remote wipe capabilities	Device must be encrypted, must use Mobile Device Management (MDM) solution, must have remote wipe capabilities if applicable
Stored on Laptop Computers	n/a	Authentication required	Laptop must be encrypted
Printed on Paper	n/a	Appropriate access controls, storage, and destruction methods	Appropriate access controls, storage, and destruction methods
Backup and Archival Storage	n/a	Consider Encryption	Must be encrypted
Storage Media Retirement/Surplus	n/a	Must be securely wiped	Must be destroyed
Storage Media Disposal	No restrictions (Optional)	Shredding or secure disposal	Shredding or secure disposal
Storage Media Sanitization	Not Required (Recommended)	Mandatory sanitization	Mandatory sanitization

Table 3 Example Data Controls

DATA TYPES REFERENCE

The following table lists common data types along with authorities that protect them, if applicable. This is not an exhaustive list of every data type an agency may encounter or every legal authority that applies.

Data Type	Description / Authority	Citation / Reference
Open – Public Record	North Dakota Open Records	NDCC 44-04
CJIS	Criminal Justise Information	28 U.S.C. §534 and 28 CFR Part 20 CJIS Security Policy

Data Type	Description / Authority	Citation / Reference
FTI	Federal Tax Information / IRS	Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies – *Safeguards for Protecting Federal Tax Returns and Return Information*
HIPAA	Health Insurance Portability and Accountability Act	NIST Special Publication 800-66: *An Introductory Resource for Implementing the HIPAA Security Rule* SP 800-66 Rev. 1
PCI	Payment Card Information	Information Supplement: PCI DSS Risk Assessment Guideline
PII	Personally Identifiable Information	NIST Special Publication 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information* NIST SP 800-122
SSA Data	Social Security Administration provided information (PII)	Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA Administration (Provided by SSA upon completion of formal agreement)

Table 4 Data Types

REVISION HISTORY

Date	Version	Description of Change
05/12/2023	0.6	Final Draft
05/16/2023	0.6	Final Draft
05/16/2023	1.0	Final Version