# Data Policy Template

## PURPOSE

All [Organization] departments collect and use data to inform decision-making and service delivery, spur innovation and collaboration, and enable civic engagement and transparency. Data are a critical resource for achieving [Organization] goals and operations.

The purpose of this policy is to recognize both the value data have in delivering the best outcomes for the [Organization], and the responsibility each department has in properly using, managing, and securing data to achieve those outcomes.

## POLICY

The [Organization] employs data practices in a manner that reflects the following values:

Customer Service — Use data in a manner to support consistent, professional, and continuously improving community services.

Respect— Ensure all data are gathered and used for equitable and transparent purposes and managed by established records management and privacy considerations.

Integrity — Classify data based on privacy, confidentiality, ownership, and security concerns, and manage and secure all data in alignment with classification schema.

Collaboration - Share data across departments and with [Organization] partners and the public to enable purposeful collaboration.

Innovation — Pursue and apply the latest advancements in data gathering, analysis, privacy, and security strategically.

To that effect, this policy defines high-level principles for the proper use, management and security of all data used by individuals on behalf of the [Organization]. It also establishes a framework for roles and mechanisms to implement those principles. The department will support implementation of this policy through roles, guidance, processes, technology, and training.

## POLICY DEFINITIONS

### [Organization] Data

[Organization] Data are defined as up-to-date statistical or factual information (1) in alphanumeric form reflected in a list, table, graph, chart or other non- narrative form, that can be digitally transmitted or processed; and (2) regularly created or maintained by, or on behalf of, the [Organization] and/ or department. Data in this context does not include documents, whether draft or final, e-mails, working papers, or documents with similar purpose.

### Criminal Justice Information Services (CJIS)

Criminal Justice Information is the abstract term used to refer to all the Federal

Bureau of Investigation (FBI) CJIS-provided data necessary for law enforcement

agencies to perform their mission and enforce the law, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information [PII]), and case/incident history data. In addition, CJIS refers to the FBI CJIS-provided Data necessary for civil agencies to perform their mission, including, but not limited to data used to make hiring decisions. Transaction control type numbers when not accompanied by information that reveals CJI or PII are exempt from the protection levels required for CJI.

### Dataset

A collection of related data that is composed of separate elements that can be

manipulated as a unit.

### Data Breach

A Data Breach is the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PII maintained by a person, commercial entity or governmental entity.

### Data Processing

A series of operations on data to retrieve, transform or classify information, oftentimes manipulating it to produce meaningful information.

### Health Insurance Portability and Accountability Act (HIPAA)

HIPAA data, or protected health information (PHI), is considered to be individually

identifiable information relating to the past, present, or future health status of an

individual that is created, collected, transmitted, or maintained by a HIPAA- covered entity in relation to the provision of healthcare, payment for healthcare services or use in healthcare operations.

### Metadata

Information describing the characteristics of data including structural Metadata

describing data structures (e. g., data format, syntax, and semantics), descriptive

Metadata describing data contents (e. g., address, date of birth), and specific acceptable uses or constraints on data use (e.g., data classification).

### Payment Card Industry (PCI)

Payment Card Industry Data includes credit card data, cardholder information, and data artifacts generated during the

acceptance, processing, storage, or transmission of credit card data.

### Personally Identifiable Information (PII)

Personally Identifiable Information are data defined by the 2018 Colorado Privacy Law as protected. PII are information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. This data includes a combination of an individual' s first name or first initial, last name and any of the following:

* Social Security number
* Driver' s License number or Identification Card number
* Student, military, or passport identification number
* Medical information
* Health insurance identification number
* Biometric data (e. g., fingerprints, iris recognition, retinal scans)

This data also includes the following combinations:

* An individual's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account
* An individual's account number or credit or debit card number in combination with any required security codes, access code, or password that would permit access to that account

PII does not include information that is lawfully made available to the public

from government records or widely distributed media.

### Regulatory Requirements

Regulatory Requirements are rules issued by a governing body, which may carry penalties for non-compliance, that are intended to manage industry specific risks.

### Security Controls

Security Controls are safeguards applied to an information system or an organization designed to protect confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

## SCOPE

This policy applies to all [Organization] data, as defined in **Section III Policy Definitions**.

This policy applies to all people who have access to [Organization] data to perform work on behalf of [Organization]. This policy defines those roles specifically responsible for establishing and executing the standards and processes defined herein for all [Organization] departments. However, all elected officials, boards and commissions, full- and part-time [Organization] employees, contracted consultants and suppliers, and other trusted partners working on behalf of [Organization] are responsible for handling data in accordance with this policy.

This policy supports existing [Organization] policies and relevant laws and regulations that govern how [Organization] manages, retains and releases records, shares public data, and secures its technology architecture. Section VI Policy Requirements, A. Law and Regulatory Compliance lists those specific [Organization] policies, laws, and regulations. By establishing the data use, management, and security principles within this policy, [Organization] can better prepare itself to execute such responsibilities fully and efficiently.

## [Organization] ROLES AND RESPONSIBILITIES

### IT Steering Committee

The purpose of the IT Steering Committee (ITSC) is to provide guidance and oversight for how the [Organization] procures and implements technology. The ITSC is a standing committee established by [Organization] executive leadership and responsible to [Organization] Manager's Office, [Organization] department leadership and the residents that [Organization] serves. The ITSC is the primary sponsor of this policy and authority on its implementation within [Organization]. The ITSC plays a specific role in assessing and determining if the collection of certain data or performance of certain data practices surpasses acceptable risks or conflicts with established [Organization] values and policies.

### Data Program Manager

The Data Program Manager is the primary executor of this policy within [Organization]. This Chief Innovation and Technology Officer assigns this role. The Data Program Manager is responsible for working with key advisers (e. g., ITSC, Chief Information Security Officer, [Organization] Records Manager) and [Organization] departments to develop and apply the roles, guidance, processes, technology, and training necessary to implement this policy's requirements. The Data Program Manager is responsible for working with Data Stewards and Data Custodians, who will be the Data Program Manager's primary contacts in implementing the policy's principles within a department.

### Chief Information Security Officer

The Chief Information Security Officer (CISO) is a key advisor to this policy's

implementation across [Organization] through the role's existing responsibilities securing [Organization] information technology systems and infrastructure in accordance with [Organization]'s Technology Security Policy.

### [Organization] Records Manager

[Organization] Records Manager is a key advisor to this policy's implementation across [Organization] through the role's existing responsibilities directing and managing the organization, maintenance, distribution, use, and retention of [Organization] records in accordance with the requirements of applicable law, [Organization] policies, best records management practices, and highest ethical standards.

### Data Steward

Each department selects a Data Steward to work with the Data Program Manager to coordinate the department's efforts to implement this policy. Departments can have multiple Data Stewards if needed. The Data Steward's primary responsibilities are to maintain a comprehensive inventory and classification of his or her department's [Organization] data, and work with the Data Program Manager to implement this policy's requirements for those data sources and Datasets.

### Data Custodian

The Data Custodians are optional roles identified by Data Stewards to serve as subject matter experts on how data are collected, transported, processed, stored, and retained within the departments, and support the department's implementation of this policy. This could include knowledge about the technical environment and database structure. If external suppliers or other partners provide these functions, the Data Custodian may be the program, project, or contract manager, i.e., a [Organization] staff member who has direct knowledge of the data use, management, and security.

### Data Users

All other [Organization] staff, suppliers, and partners who handle [Organization] data need to do so as outlined within this policy and as guided and trained by the relevant roles above.

## POLICY REOUIREMENTS

### Law and Regulatory Compliance

[Organization] must use, manage, and secure all [Organization] Data in accordance with all applicable data, records management and privacy policies, laws, and regulations. Those include:

* [Organization] Access to Public Records Policy
* [Organization] Management of [Organization] Records Policy
* [Organization] Open Data Policy
* [Organization] Technology Security Policy
* [Organization] Electronic Communications Retention and Auto Delete Policy
* [Organization] Litigation Hold and Data Preservation Policy
* Colorado Open Records Act (CORA)
* Colorado Criminal Justice Records Act (CCJRA)
* Colorado privacy laws pertaining to Personally Identifiable Information (PII)
* Children' s Online Privacy Protection Act of 1998 (COPPA)
* Health Insurance Portability and Accountability Act of 1996 (HIPAA)
* Critical Infrastructure Information Act of 2002 (CII)
* Payment Card Industry Data Security Standard (PCI DSS)
* FBI Criminal Justice Information (CJI) Security Policy

### Data Classification

Classification of data by sensitivity supports the process of determining who should have access to [Organization] Data and how that data should be used, managed, and secured.

The Data Program Manager and CISO will work with Data Stewards to classify all departments' data and establish rules and proper use of data based on that classification. This classification should be documented to readily inform [Organization] Data access management.

Note that the criteria for classifying data are purposely different from those criteria used to assess whether records can be made public in response to CORA requests. Data classification informs how data should be used, managed, and secured within [Organization], while CORA criteria inform what data could be released in response to an open records request.

#### Classification Categories

All [Organization] Data must be classified into one of the following three categories:

* + 1. **Protected** - Any Dataset or portion thereof to which [Organization] may deny access pursuant to established [Organization] policy, [Organization] Charter, Federal, or State law, privacy laws, copyright, patent, trademark, confidentiality agreement or any other law, rule, regulation, or common law privilege. This includes data that [Organization] is prohibited from disclosing by operation of law, including CJIS, HIPAA, and PCI.
		2. **Sensitive** - Any data which, if shared by [Organization], could raise privacy, confidentiality, proprietary, or security concerns or have the potential to jeopardize health, safety, or welfare to an extent that is greater than the potential public benefit of sharing that data. Access to sensitive data should be determined by the stated purpose of the individual requesting access, and whether that purpose is in line with the data's intended use, law and regulatory compliance, and [Organization] values. Examples include certain PII, personnel records, physical security access logs, and investigative data.
		3. **Public** - All data generated or received by [Organization] which are not classified as protected or sensitive data, and which have been prepared for release to the public is considered public data. Refer to [Organization]'s Open Data Policy for more definition and guidance.

#### Determining Classification

The Data Program Manager and CISO will maintain guidance for departments to classify data, document such classification, and establish Security Controls accordingly.

There is no perfect system for determining data classification. In some situations, the appropriate classification may be obvious, such as when [Organization] is required by law to secure certain types of data (e.g., PII). If the appropriate classification is not easily determined, Data Stewards and Data Custodians should work with the Data Program Manager and CISO to make a reasonable determination.

#### Reclassification

Significant events that impact the sensitivity of data may trigger a need to reclassify data. [Organization] should react to events such as a security incident, business process change, migration to a new platform, or the establishment of new laws or regulations with a reevaluation of relevant data's classification. If a determination is made that the classification of certain data has changed, an analysis of Security Controls should be performed to determine whether existing Security Controls are consistent with the new classification. If gaps are found in existing Security Controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

### Assessing Risk of Data and Data Practices

[Organization] recognizes that certain data and practices manipulating data can contain inherent risks and biases which run counter to [Organization] values. To mitigate these concerns and provide guidance to departments, the ITSC will establish the means to assess and determine if the collection of certain data or performance of certain data practices create such conflicts (i. e., surpasses acceptable risks or otherwise conflicts with established [Organization] values and policies). Based on these determinations, the ITSC will identify areas for the Data Program Manager to provide further guidance and training as needed to properly inform [Organization] departments' use of such data or data practices.

Topics the ITSC may need to consider for this purpose include:

* Artificial Intelligence — [Organization] data may be used to train [Organization]-operated or third-party artificial intelligence to facilitate business processes or decision-making. The quality of the results of artificial intelligence processes can be strongly impacted by biases in the training data, and/or the technology developer. Decisions derived from artificial intelligence processes must be assessed to ensure they reflect the [Organization]'s values, and business processes built to augment artificial intelligence with human intelligence and analysis.
* Supplier Technology — It is important the [Organization] retains knowledge and control of the types of data collection and processing technologies being applied on behalf of [Organization]. Contracts should confirm that [Organization] owns all data collected or created on behalf of [Organization]. Per [Organization]'s Technology Security Policy, [Organization] technology must be set up to control access to, retain, and dispose of [Organization] Data in accordance with [Organization]'s Data and records management policies and Regulatory Requirements relevant to that data. As such, supplier solutions should be evaluated and required to abide by this policy and decisions made by the ITSC around data and data practices. Supplier proposals should clearly articulate proposed technology's data approaches and when possible, provide alternatives for [Organization] to select upon contract award.
* Data Collection in Public Space — Technology advancements enable significantly expanded abilities to collect more types and more amounts of data. There are many possible uses of this data to make [Organization] services more efficient and effective, ranging from public safety to public engagement. The ITSC will need to weigh collection and use of such data with community security and privacy.

### Data Management

Data management is essential to ensure that the highest quality data is collected, maintained, used, and made available for [Organization] staff, partners, and the public. This section outlines principles to be implemented by the Data Program Manager and [Organization] departments.

#### Data Management Plans

Each department should consider the development of data management plans to document the handling of data during specific projects or for a specific program's systems or databases. Data management plans may include the purpose of the project or program's data, Metadata or data dictionary, data classification, data change control procedures, data sharing and transmission requirements, Data Processing and analytics approaches, data storage and retention, etc.

#### Data Source and Dataset Inventorying

Data inventorying and making those inventories readily accessible helps make data more discoverable. The Data Program Manager will work with Data Stewards to maintain a comprehensive inventory of departments' [Organization] data. This inventorying should include data classifications and other necessary Metadata associated with data sources and Datasets. This inventory must be regularly maintained, with at least annual assessments by the Data Program Manager and Data Stewards.

#### Metadata Documentation and Standardization

[Organization] departments collect similar [Organization] Data (e.g., individuals' addresses or dates of birth) to achieve their own service delivery or operations, but the format or syntax of that data may be different between department or even systems within a single department. When similar [Organization] Data are collected across multiple departments or exists in multiple technology systems, [Organization] departments should collect and maintain standardized Metadata to ease data sharing and analyses across those departments or systems. The Data Program Manager will work with Data Stewards to structure such standardization and integrate the approach into data source and Dataset inventorying processes.

#### Data Change Control

Data and the methods, standards, and tools [Organization] departments use to collect, store, and retain data change over time. Those changes must be effectively documented to inform ongoing and future use of that data. [Organization] departments should employ data change control practices to manage and document such changes to data. The Data Program Manager will provide guidance and templates to Data Stewards to inform how such data change control could be best applied in their departments.

#### Data Quality

Data quality refers to data achieving the purposes for which its collection and use are intended. Quality can be considered by the overall consistency and trustworthiness of data. Higher quality data are more valuable and more effective when used for decision-making.

##### Data Quality Audit

The Data Program Manager will aid Data Stewards in conducting data quality audits to identify problems and determine ways to address the root cause of those problems. All data quality issues should be documented for data users' awareness and, within reason, addressed promptly.

##### Data Quality Feedback Channels

The Data Program Manager will aid Data Stewards in establishing appropriate feedback channels for data users to identify data quality issues and when needed conducting audits to validate any issues, determine what would need to be done to address those issues, and establish a plan for remediation.

#### Data Sharing

Effective internal (i.e., between [Organization] staff) and external (i.e., with non-[Organization] staff) data sharing is crucial for transparency, accountability, collaboration, and innovation. Sharing data in near-real time within [Organization] should be a default practice, but for data classified as protected or sensitive, sharing methods should be regularly reviewed to ensure they are secure and reliable. The Innovation and Technology (IT) Department can assist with recommending and setting up secure methods of sharing protected and sensitive data with internal and external parties.

##### Sharing Protected Data

Internal Sharing: Participants in protected data sharing are required to use sharing methods that do not create copies of the data outside of the system of record as defined by [Organization]'s Management of [Organization] Records Policy processes. The best way to accomplish this is to link to the system of record. Sharing Protected data through unprotected methods, such as email, puts that data and [Organization] at significant risk.

External Sharing: Sharing of any protected data requires a written and signed contract, Memorandum of Understanding, or Data Sharing Agreement. These documents should clearly define the expectations and responsibilities of each entity to safeguard [Organization] data and the penalties if they fail to do so. In all cases, it is required that each non-[Organization] staff individual handling the data sign an executed Non-Disclosure Agreements (NDA). Participants in protected data sharing are required to select secure and encrypted sharing methods such as those described in Section 7, Data Transmission.

##### Sharing Sensitive Data

Internal Sharing: Participants in sensitive data sharing are encouraged to select sharing methods that do not create copies of the data outside of the system of record as defined by the [Organization]'s Management of [Organization] Records Policy processes. The best way to accomplish this is to link to the system of record. Sharing sensitive data through unprotected methods, such as email, puts that data and [Organization] at significant risk.

External Sharing: External sharing of any sensitive data may require a written and signed contract, Memorandum of Understanding, or Data Sharing Agreement, per guidance from [Organization] Attorney's Office. These documents should clearly define the expectations and responsibilities of the entity to safeguard [Organization] data and penalties if they fail to do so. In all cases, it is required that each non-[Organization] staff individual handling the data sign an executed NDA. Participants in sensitive data sharing are required to select secure and encrypted sharing methods such as those described in Section 7, Data Transmission.

##### Sharing Public Data

Internal and external sharing of public data is encouraged. [Organization]'s Open Data Policy details the process for sharing public data. [Organization] staff should also consider making recurring data sharing occur automatically and in near-real time through the [Organization]'s Open Data Catalog.

##### Techniques to Desensitize Data

[Organization] staff can employ techniques (e. g., denaturing, aggregating, hashing) to desensitize data in order to share it more broadly. Such techniques require technical expertise to ensure the data are properly processed to address all sensitivity and privacy concerns. [Organization] staff should contact their Data Steward, the Data Program Manager, or the CISO if they have questions on how to desensitize data effectively before sharing.

#### Data Transmission

[Organization] data must be transmitted using methods appropriate to the specified data classification. Data Stewards or [Organization] staff with questions about which method is most appropriate should work with the Data Program Manager and CISO to make that determination.

Sharing [Organization] Data using informal methods, such as email, puts that data at significant risk. Secure and encrypted external data sharing mechanisms include Office 365 external file sharing, secure file transfer protocol (SFTP), or an IT-approved application programming interface (API).

Additionally, [Organization] departments need to take precautions ensuring dynamic, recurring, or large load data transmissions do not have any adverse impacts on technical production environments and [Organization] operations. Data Stewards and [Organization] staff can contact the CISO and IT Department for more guidance setting up those precautions.

#### Data Retention and Destruction

Retention and destruction of [Organization] Data must be performed in accordance with the Management of [Organization] Records Policy, Technology Security Policy, Electronic Communications Retention and Auto Delete Policy, Litigation Hold and Data Preservation Policy, and all other relevant regulatory and legal standards.

[Organization] staff must irreversibly erase data when data are destroyed per such policies and standards, per the [Organization]'s Management of [Organization] Records Policy. Under some circumstances, data destruction may result in associated data being orphaned. This means that records still exist but are not referenced directly by any system. To prevent the proliferation of orphaned data, all orphaned records are to be subjected to the same retention criteria appropriate to the parent data and destroyed in the same process. Data Stewards and [Organization] staff can contact the CISO and IT Department for more guidance on proper data destruction.

#### Reporting Concerns about Data

All data users must promptly report suspected data security or privacy issues, including Data Breaches, to the CISO or the IT Service Desk.

## COMMUNITY COMMUNICATION

[Organization] is committed to ensuring that our community understands this policy and how [Organization] staff execute this policy. Maintaining transparency is crucial to effective use, management, and security of data.

## POLICY COMPLIANCE

The ITSC and Data Program Manager will regularly assess [Organization]-wide progress toward the data use, management, and security principles outlined within this policy. This assessment and any resulting actions will be undertaken in coordination with Data Stewards to best mature such data practices.

## INTERPRETATION AND APPLICATION

[Organization] employees who have questions concerning the interpretation and application of this policy are encouraged to contact their department's Data Stewards and the Data Program Manager.