| **Document Field** | **Document Value** |
| --- | --- |
| Title | Responsible Data Science Policy (“Policy”) |
| Document ID |  |
| Version |  |
| Last Updated | (date) |
| Last Reviewed | (date) |
| Responsible Body |  |

# 1. Introduction

## 1.1 PRINCIPLES

[Three/Four] principles guide the responsible use of data and models by [Organization] (“Organization”). When the policy or related procedures are unclear, these Principles can be used to guide decisions.

**Principle 1**: The Organization should continuously identify and understand risks arising from its data science activities, regardless of whether the harm might be external or internal.

**Principle 2**: The Organization should use data science to contribute positively to the people, processes, and performance of the Organization.

**Principle 3**: Whenever reasonably possible, the Organization should manage risks arising from its data science activities, such as through risk avoidance, reduction, or offset, regardless of whether the harm might be external or internal.

[**Principle 4**: Whenever reasonably possible, the Organization should use data science to contribute positively to people, societies, and environments more broadly.]

## 1.2 PURPOSE

The Organization desires that its data science activities be conducted in a responsible manner that aligns with the Principles above. The objective of this Policy is to ensure that the Organization works to achieve these Principles from a technical, legal, and ethical perspective by establishing the standards, restrictions, and procedures that govern data science activities within the Organization.

## 1.3 SCOPE

This Policy applies to:

1. All data science activities, including those commonly described as statistical analysis, business intelligence, analytics, machine learning, artificial intelligence, or any other similar activities (collectively, “Data Science”)
2. All employees [and contractors] that manage or perform Data Science (“Personnel”)
3. All data that is used by Organization in the context of Data Science (“Covered Data”)
4. All models that are used by Organization in the context of Data Science (“Covered Models”), whether used on a continual basis or not

## 1.4 PROCEDURES

[POLICY OWNER] is responsible for establishing a parent Procedure and one or more Sub-Procedures to govern the process of executing on this Policy. Two types of Sub-Procedures are supported under this Policy.

### 1.4.1 Prescriptive Sub-Procedure

A Prescriptive Procedure defines the following:

1. Clear criteria regarding the transparency, use, provenance, and general nature of Covered Data and Covered Models
2. Minimum standard of transformation for attributes or Data Subjects
3. Minimum acceptance criteria for release, such as differential privacy metrics

When these standards and restrictions can be met, projects can generally proceed with little to no additional review.

### 1.4.2 Adjudicative Sub-Procedure

An Adjudicative Procedure utilizes the following:

1. A Data Science Proposal Form, to be completed by the requesting party (“Submitter”)
2. A Data Science Adjudicator (“Adjudicator”) responsible for evaluating such Data Science Proposals

Submitters complete Data Science Proposal Forms, which are then sent to the responsible Adjudicator for review. The Adjudicator, which may be an individual or a larger group such as a committee or board, may reject the proposal, request further information or modification, or approve the proposal upon review.

[POLICY OWNER] is responsible for the establishment of one or more adjudicators, who must possess relevant experience and qualifications to support the assessment of technical, legal, and ethical considerations. [POLICY OWNER] may create a single Adjudicator to review all Proposals or may create multiple Adjudicators to address one-time or recurring use cases such as industry, regulation, or geography.

## 1.5 REGULATIONS AND STANDARDS

This Policy contemplates and is intended to be compatible with the following regulations and standards, but is not intended to fully address all requirements of them:

* General Data Protection Regulation (GDPR), EU 2016/679.
* California Consumer Privacy Act of 2018 (CCPA), AB-375 or as otherwise codified and amended under the California Civil Code.
* [list other regulations and standards]

[[Additional information on related regulations and standards can be found at [POLICY KNOWLEDGE BASE].]]

## 1.6 RESPONSIBILITY

[POLICY OWNER] is responsible for developing and maintaining this Policy. The initial Policy and all subsequent updates must be approved in writing by [POLICY APPROVER]. [POLICY OWNER] is responsible for monitoring technical, legal, and ethical trends related to this Policy and must review the Policy in its entirety at least once per [POLICY REVIEW INTERVAL].

## 1.7 GUIDANCE

Personnel may contact [POLICY OWNER] with questions, comments, or concerns regarding this Policy and related Procedures at [POLICY OWNER CONTACT INFO]. [[Additional information on data handling can be found at [POLICY KNOWLEDGE BASE].]]

## 1.8 COMPLIANCE

[POLICY OWNER] is responsible for verifying compliance with this Policy and related Procedures in a manner of their choosing, including, but not limited to, hiring or contracting people or implementing processes or technology.

For Covered Data and Covered Models that are used on a continual basis or released into continuously-operating software, [POLICY OWNER] is responsible for implementing an audit strategy to verify ongoing compliance, such as by contracting third-party auditors. Covered Data and Covered Models should be audited at least once per [PROJECT REVIEW INTERVAL].

## 1.9 **EXCEPTIONS**

Any and all exceptions to this Policy and related Procedures must be approved in writing by [POLICY EXCEPTION APPROVER]. Such exceptions, including supporting justification, must be documented in [EXCEPTION LOG].

## 1.10 **VIOLATION**

Personnel found to be in violation of this Policy or related Procedures are subject to disciplinary action as outlined in the [DISCIPLINARY POLICY]. Additionally, given the nature of risks related to Covered Data, Personnel in violation of this Policy or related Procedures may be subject to additional action, including, but not limited to, termination of employment.

# 2. Standards and Restrictions

## 2.1 TRANSPARENCY

Data Science should be transparent in its intention. If the Data Subject is an individual, they must [CONSENT TO/BE NOTICED OF] Organization’s specified purpose and potential use of their data. If the Data Subject is not an individual, then the Data Owner should [CONSENT TO/BE NOTICED OF] Organization’s purpose and potential use of their Covered Data. [POLICY OWNER] is responsible for ensuring that such [CONSENT/NOTICE] is sufficiently documented.

[POLICY OWNER] is responsible for ensuring that the Organization can establish when Data Science occurs, who is performing the activities, what Covered Data or Covered Models are being used, and how the activities being performed relate to a permissible purpose.

If the Organization desires to use Covered Data for a purpose other than specified to the Data Subject or Data Owner, [CONSENT/NOTICE] must be [OBTAINED/PROVIDED] prior to performing activities.

## 2.2 DATA USE

Covered Data must only be used, disclosed, or otherwise made available for the specified purposes, except as:

* Consented to in writing by the Data Subject and, if applicable, by the Data Owner, or
* Required by law, regulation, or court order, or similar governmental compulsion.

## 2.3 PROVENANCE

Data Science should establish and maintain clear provenance for Covered Data and Covered Models. [POLICY OWNER] is responsible for ensuring that Procedures exist to determine and document such provenance. Provenance is required to establish facts related to technical, legal, or ethical risk assessments, including information such as the means of collection or the Data Subject/Data Owner.

## 2.4 ETHICS

The Organization desires to avoid activities that are either unfair or unethical in their means or ends. The Organization acknowledges that Data Science can meet legal standards and requirements while still involving unfair or ethically-undesirable processes or outcomes such as bias. [POLICY OWNER] is responsible for ensuring that Procedures exist to identify, understand, and manage ethical concerns in a manner consistent with other risks.

## 2.5 SUPPLY CHAIN

Whenever reasonably possible, the Organization should align standards, restrictions, and procedures under this Policy with the standards, restrictions, and procedures of its supply chain. [POLICY OWNER] is responsible for working with [CONTRACTING/PROCUREMENT OWNER] to monitor and manage towards this goal.

## 2.6 CONCEPTS AND TECHNIQUES

[POLICY OWNER] is responsible for researching and documenting concepts, especially those related to privacy and fairness acceptance criteria, and techniques, especially those explicitly prohibited or approved from a privacy or explainability perspective. Whenever reasonably possible, the Organization should align the technical concepts and techniques used under this Policy with leading standards and research in privacy and fairness generally. Such documentation can be found in this policy under the Concepts and Techniques Inventory.