IRMA Initiative for Responsible Mining Assurance

Data Governance Policy

Version 20251103

November 2025

Responsibility for This Policy

IRMA holds responsibility for this document and its contents.

Version No.	Date	Description of Action or Amendment
v20250926	September 2025	First publication, approved by the Board of Directors
V20251103	November 2025	Minor procedural clarification by the IRMA Secretariat

1. Purpose and Scope

1.1. Purpose

This policy establishes the framework for managing data received or created by the Initiative for Responsible Mining Assurance (IRMA). Its purpose is to ensure that IRMA's data is managed securely, ethically, and efficiently. It provides operational clarity and defines accountability for data stewardship across the organization.

1.2. Scope

This policy applies to all data, regardless of format, created or handled by IRMA personnel, Board or committee members, approved audit firms, working groups, and other participants in IRMA processes. It governs data within all IRMA's core information systems, including assessments and the assurance program, monitoring and evaluation, risk management, stakeholder engagement, organizational administration, and other purposes. This policy is guided by ISEAL's Code of Good Practice for Sustainability Systems V1, Section 4. It is complemented by and should be read in conjunction with IRMA's Confidentiality Policy and Privacy Policy.

2. Data Classification

All data must be classified into one of the following four categories to determine appropriate handling, access, and security protocols.

- **Public:** Information intended for unrestricted access and public consumption. Disclosure carries minimal risk.
  Examples: Final audit reports, public statements, website content, press releases.
- **Internal:** Data for general use by IRMA personnel, Board of Directors members, and authorized partners for day-to-day business operations. Unauthorized disclosure would not cause significant harm but is not intended for the public.
  Examples: Secretariat meeting minutes, project plans, drafts not containing sensitive information.
- **Confidential:** Non-restricted sensitive information that, if disclosed without authorization, could harm IRMA, its partners, or stakeholders.
  Examples: membership inquiries and applications, sensitive stakeholder communications.
- **Restricted:** IRMA's most sensitive data, requiring the highest level of security and strictest access controls. Unauthorized disclosure could result in significant harm, legal liability, or breach of trust with critical stakeholders.
  Examples: draft audit reports, data subject to non-disclosure agreements.

3. Data Roles and Responsibilities

Accountability is central to data governance. The following roles are established:

- **Data Owner:** The Data Owner is a senior-level individual who has ultimate accountability for the data within their domain. This person is responsible for the overall classification and usage of their assigned data. They make decisions about access permissions, security controls, organization, and the lifecycle of the data, working closely with the Data Custodian and Data Steward to ensure the data is accurate, secure, and compliant with relevant regulations. Data Owners are assigned by IRMA's executive leadership according to their functional domains of responsibility (e.g., the Director of Assurance is the Data Owner for assurance program data).
- **Data Steward:** An individual or team responsible for the day-to-day implementation of this policy for a specific dataset or system, working closely with the Data Owner. Their duties include ensuring data

accuracy, consistency, and integrity. They may define and implement data quality rules and lead periodic reviews to ensure data quality is maintained. Not all types of data will have a Data Steward.

- **Data User:** A Data User is any individual who accesses, processes, or uses data as part of their job function. Their responsibility is to adhere to the organization's data governance policies, including proper handling, use, and protection of data. They must understand and follow rules regarding data access, sharing, and disposal.
- **Data Custodian:** The Information Systems Director is the Data Custodian, a technical role responsible for the secure storage, maintenance, and protection of data. They manage the infrastructure where the data resides, including databases and cloud storage. Their responsibilities include implementing the security controls and access permissions as defined by the Data Owner, and ensuring the technical integrity of the data. The Data Custodian is responsible for recording and maintaining information about types of data, classifications, data roles, and access controls. They work closely with Data Owners, Stewards, and Users to ensure full implementation of this policy.

4. Access Control

Access to data is governed by the Principle of Least Privilege, which grants individuals only the access required to perform their job functions. Access is decided by the relevant Data Owner in cooperation with appropriate personnel. Controls are implemented via platform-specific capabilities and established and/or reviewed by the Data Custodian in cooperation with the Data Owner. The Data Custodian maintains an ongoing record of the different types of data, assigned roles, access control, and their storage locations.

5. Data Quality and Integrity

IRMA is committed to maintaining high-quality data. Data Stewards are responsible for periodic data reviews to ensure accuracy, completeness, and consistency. Review periods will be set by the Data Owner in accordance with accepted best practice.

Data collected and managed by IRMA should be essential for its mission and operations. The organization will avoid the collection and ownership of unnecessary audit data to minimize risk and ensure efficiency. Data Owners and Data Stewards, in cooperation with the Data Custodian, are responsible for ensuring that only data required for IRMA's core functions and business operations is retained.

6. Data Inventory

The Data Custodian, in collaboration with all Data Owners, will establish and maintain a Data Inventory.
This inventory will address IRMA's primary data domains, specifying for each:

- The Data Owner
- The physical or logical location of the data
- A description of who has rights to the data
- The conditions under which data is made available, both internally and externally

The inventory will be reviewed on an annual basis.

7. Data Security and Legal Compliance

IRMA will protect its data from unauthorized access or breach through a multi-layered security approach. Ensuring that data is accurate, secure, and compliant with all relevant regulations is the shared responsibility of Data Owner, Data Steward, and Data Custodian.

- **Endpoint Security:** All IRMA-managed devices are managed through a mobile device management (MDM) system with enforced security policies.
- **Access Security:** All IRMA-managed information systems services will operate in accordance with Least Privileged Principles and implement standard security practices, including Multi-Factor Authentication (MFA).
- **Training and Capacity-Building:** All personnel who hold data-related roles will undergo cybersecurity training and testing on a periodic basis. The training will be administered by the Data Custodian.
- **Data Handling by Third Parties:** Contracts with third parties handling data on IRMA’s behalf must require them to implement adequate data

security procedures that ensure confidentiality and integrity, safeguards against unauthorized use, compliance with applicable law, and appropriate security measures.

- **Legal Compliance:** IRMA will comply with all applicable legal requirements regarding data management as outlined in its Privacy Policy, Confidentiality Policy and Document Retention and Destruction Policy.

8. Policy Review and Maintenance

This policy will be reviewed annually and revised at least once every five years.