INFORMATION GOVERNANCE POLICY

Effective: September 1, 2020

Purpose of Policy

This Policy is intended to establish the principles of information governance for the protection, management and disposition of Catalyst information to meet Catalyst's legal, regulatory and business operational requirements.

Application of Policy

This Policy applies to all Catalyst employees, contractors, vendors and agents with access Catalyst information.

Policy

All individuals with access to Catalyst information must identify, classify, protect, retain and dispose of Catalyst information in accordance with fundamental information governance principles.

Identification

1. Catalyst's structured information stored in applications/databases shall be inventoried and tracked by Catalyst's Information Technology (IT) Department based on:
    a. Type of data stored/passed
    b. Storage location
    c. Data transfer methods, recipients and region
    d. Business, data or application owner
2. Catalyst's unstructured information must be stored in Catalyst-approved storage locations inventoried by the IT Department.

Classification

1. Information (structured & unstructured) must be classified with one of the Catalyst Classification Categories set forth below in accordance with the Catalyst Data Classification Standard.
    a. When information falls into more than one classification category, the most restrictive classification label must be applied.

2. The business, data or application owner (Information Steward) is accountable for the appropriate classification of information.

Catalyst Classification Categories

Restricted	Internal	Public
Information that is sensitive within Catalyst and is intended for use only by specified groups of employees. Restricted data includes any information that Catalyst has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner.	Information that is generally available to employees and approved non-employees.	Non-sensitive information available for external release.

Protection

1. Based upon its value, use and purpose, information must be protected according to its Catalyst Classification Category from the time of creation or receipt through the end of its lifecycle per the following protection controls matrix.

		Restricted	Internal	Public
Access	System and Application data requires authentication to ensure that only authorized individuals have access to and can modify this data. Electronically stored documents should only be accessed by individuals who have a legitimate business need to view, edit or use the data.	X	X	
Secure Disposal	Electronic data must be securely wiped from storage media prior to disposal, or the media must be destroyed.	X	X	
Secure Storage	Application data must be processed and stored in a Catalyst-approved secure location or device and transported on secure networks (see Physical Security Policy). Documents (electronic and physical) should be stored in approved locations.	X	X	

Encryption in Transport	Application data must be encrypted when transported on public or wireless networks. Passwords must be encrypted in transport regardless of the underlying network. Electronic documents sent via email must be encrypted using available technologies in Outlook.	X	X	
Encryption at Rest	Stored application data and electronic documents must be encrypted.	X		
Logging and Alerting	Key systems data is logged and monitored when accessed.	X		

Retention

1. Information must be retained per its Catalyst retention period requirement based on legal or regulatory requirements, including legal hold and operational business needs, in accordance with the Catalyst Data Retention Standard. In the absence of a defined retention period, a default or minimum retention of 180-day will apply.

Disposition

1. Information not subject to a Catalyst retention requirement should not be retained longer than the defined retention period outlined in the Catalyst Data Retention Standard.
2. Personal information must be securely disposed when no longer necessary to support its intended purpose per Catalyst's Privacy Policy and in compliance with applicable privacy laws.
3. In the event of anticipated or actual litigation, a government investigation, an audit or as warranted by any other legal matter, a legal hold will be implemented ty the Legal Department to preserve information that is relevant to the matter. Any information under legal hold must be retained until the legal hold is released in writing by the Legal Department. You may check whether you are subject to a legal hold by emailing legal@catalyst.org.
4. Securely dispose of information once the retention period requirement has expired.
    a. Perform regular reviews (at least annually) of information for relevance/usefulness.

Data Protection Principles

The aim of the Policy is to comply fully with internationally accepted principles and requirements for data protection. To meet these requirements, Catalyst has adopted the following general principles for data protection and processing to govern the use, collection, and transfer of personal data, except as specifically provided by this Program or as required by applicable laws:

Fairness and lawfulness

In processing personal data, Catalyst must protect the individual rights of data subjects and process such data fairly and in accordance with legal provisions.

Restriction to a specific purpose

Catalyst may process personal data only for the purposes for which it originally collected such data. Subsequent changes to the purpose are possible only to a limited extent. Such changes may take place by virtue of a contractual agreement with the data subject, consent given by the data subject, or pursuant to specific legislation.

Transparency

The data subject must be informed of how Catalyst manages his or her data. As a matter of principle, personal data must be collected directly from the data subject concerned when practicable. When collecting the data, the data subject must either be aware of, or be informed of the following:

- The identity of the data controller;
- The purpose for which the data is being processed;
- The recipients or categories of recipients of the data;
- The right to access and rectify personal data; and
- That data collected for marketing purposes is voluntary.

In addition, various jurisdictions may impose additional or differing requirements regarding the content and scope of this information. Such requirements might include, for example, information that a data subject has the right to object to contact made for marketing and advertising purposes.

Current and Accurate data

Personal data must be current and accurate when stored. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, or supplemented.

Data requiring special protection

Catalyst will not process “sensitive data” or “special categories of data” (as defined by applicable law) unless:

- Specifically authorized or required by law or the data subject gives express consent; or
- Required for preventive medicine, medical diagnosis, or health care.

Transfers to third parties

Where Catalyst transfers personal data to another entity, country, or territory, Catalyst will take reasonable and appropriate steps to maintain the required level of data protection.

Automated Decision Making

Catalyst personnel who engage in any decision-making based solely on the automated application of pre-determined rules must disclose this practice to the data subjects. The data subject must be given the opportunity to (i) review the logic used by the automated system, (ii) supplement the automated system with additional data, and (iii) obtain review of the automated decision by an individual.

GDPR

For the transborder flow of data originating from the European Economic Area (EEA) or from countries that require an adequate standard of protection for transborder data flows, the party importing the data must comply with the national legislation in force in the country from which the data originated when processing such data. This does not apply for data flows within the EEA or for transborder data flows into non-EEA countries that have been deemed by the European Commission to have an adequate level of data protection.

The notification requirements for data processing set out in the laws of individual nations must be met. Catalyst personnel operating in jurisdictions other than the United States must check whether and to what extent such notification requirements exist.

Violations of Policy

- **Non-Compliance.** An employee who violates this Policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Data Classification Standard
- Data Retention Standard
- Physical Security Policy
- Privacy Policy

Definitions and Terms

- **Structured Data:** Information that has been organized into a formatted repository, typically a database, so that its elements can be made addressable for more effective processing and analysis.
- **Unstructured Data:** Information that either does not have a predefined data model or is not organized in a pre-defined manner. This data is usually not easily searchable, including formats like text files, audio, video, and social media postings.

Administration of this Policy

- **Questions.** You are encouraged to ask any questions you may have about this Policy. To learn more, please contact secure@catalyst.org.

- **Reporting.** It is important that you immediately report any suspected violation of this Policy by a Catalyst employee or third party to your manager or to HR. All good faith allegations of violations of this Policy will be fully and confidentially investigated.
- **Exception to Standard.** Limited exceptions to the Policy may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Policy. Any request for an exception to the requirements of this Policy must be submitted to the Information Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.
- **Applicability.** This Policy applies globally unless contrary to local laws and regulations. Operations in different countries may have more stringent policies or implementing procedures where required by local law. In the event of a conflict, these more stringent policies or implementing procedures will take precedence.

Revision History

Date	Name	Description	Responsibility
09/01/2020	James Mbassa	Initial release.	Owner