DATA CLASSIFICATION STANDARD

Effective: September 1, 2020

Due to the vast amounts and criticality of information throughout Catalyst, all staff members have an important role to play in protecting, and a responsibility to protect, the information entrusted to their care. All who access sensitive information are expected to familiarize themselves with this Data Classification Standard and to consistently follow it in their business activities. Sensitive information is classified as either “internal” or “restricted” information (defined below).

Purpose of Standard

This Standard is intended to protect the confidentiality, integrity and availability of Catalyst data. Consistent use of this data classification system will facilitate contractual, legal, and regulatory obligations and help keep the costs for information security to a minimum. Without consistent use of this data classification system, Catalyst risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

Application of Standard

This Standard applies to all information in Catalyst’s possession or under its control. For example, information entrusted to Catalyst by Supporter organizations, clients, credit card payers, vendors, partners, and others must be protected with this data classification standard. Staff members are expected to protect third party information with the same care that they use to protect Catalyst information. The terms "data," "information," "knowledge," and "wisdom" are used interchangeably in this Standard and other Catalyst policies and standards.

Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, and what purpose(s) it serves. Although this Standard provides overall guidance, to achieve consistent information protection, Catalyst staff must apply and extend these concepts to fit the needs of day-to-day operations.

Technical Requirements

- **Classification:** All data must be assigned an appropriate sensitivity classification as defined immediately below.
    - **Public** - Non-sensitive information available for external release.

- **Internal** - Information that is generally available to employees and approved non-employees.
- **Restricted** - 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.
- Default Label: The majority of Catalyst information falls into the “Internal” category. For this reason, it is not necessary to apply a label to “Internal” information. Information without a label is therefore by default classified as Internal Use Only.
- Public Information Labels: All Public information must be labeled "Approved for Public Release" along with the date when the Information Steward declared the information public.
- Restricted Label: All Restricted data must be labeled accordingly and stored in a manner and/or location commensurate with its classification.

- **Information Steward:**
  - The Information Technology department does not ‘own’ Catalyst data. This stewardship is the responsibility of the head of a functional area (e.g. Accounting, HR, Legal, Marketing, etc.).
  - All information possessed by or used by an organizational unit within Catalyst must have a designated Information Steward.
  - The Information Steward must identify and classify the information for which they are responsible.
  - Information Stewards are responsible to store all data in locations that support retention and disposition standards per the Records Retention Standard.

Access Controls:

- Need to Know: One of the fundamental principles of information security is the "need to know."
  - Information should be disclosed only to those people who have a legitimate business need for the information. This principle applies to private employee information such as medical histories, just as it applies to client data or proprietary corporate information such as plans for a new product.
  - All sensitive information must be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. These controls must not only control access based on the need to know, they must also log which users accessed sensitive data.
- Mixed data: If information with a higher sensitivity classification is moved to a location with a lower sensitivity classification, the location with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity classification. In

general, because it increases handling costs as well as operational complexity, the commingling of information with different sensitivity classifications is discouraged.

- Access Granting Decisions: Access to sensitive information must be provided only after the express authorization of the Information Steward has been obtained. All requests for information must be referred to Stewards or their delegates. Absent such approval, all requests must be denied.

- No Read-up Permissions: Those who have been authorized to view information classified at a certain sensitivity level must be permitted to access only the information at this level and at less sensitive levels.

- No Unauthorized Downgrading: Catalyst staff must not move information classified at a certain sensitivity level to a less sensitive level unless this action is part of a formal declassification or downgrading process approved by the Steward.

- **Third Party Interactions:**

  - Third Parties and the Need to Know: Unless it has specifically been designated as Public, all Internal information must be protected from disclosure to third parties. Third parties may be given access to Internal information only when a demonstrable need-to-know exists, and when such a disclosure has been expressly authorized by the relevant Information Steward.

  - Disclosures to Third Parties and Non-Disclosure Agreements: All disclosures of sensitive information to third parties must be accomplished via a signed non-disclosure agreement (NDA) which includes restrictions on the subsequent dissemination and usage of the information.

  - Disclosures from Third Parties and Non-Disclosure Agreements: Catalyst staff must not sign non-disclosure agreements provided by third parties without the advance authorization of Catalyst's Legal Department or other parties approved by the Chief Executive Officer.

  - Unless a staff member has been authorized by the Information Steward to make public disclosures, all requests for information about Catalyst and its business must be approved by the CEO, or CFAO. Such requests include questionnaires, surveys, newspaper interviews, and the like. This Standard does not apply to sales and marketing information about Catalyst products and services, nor does it pertain to calls made by Catalyst to obtain customer support.

- **Steward Notification:**

  - If sensitive information is lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the Information Steward and the VP of Information Technology must both be notified immediately.

- **Removal from Offices**

- Sensitive information may not be removed from Catalyst premises unless there has been prior approval from the relevant Information Steward. An exception is made for authorized, and IT-managed, off-site back-ups.

- Removal includes physical removal in addition to electronic removal, such a copying information from Catalyst-approved storage to non-approved locations or media.

Violations of Standard

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

Related Standards, Policies and Processes

- Information Governance Policy

- Record Retention Standard

Definitions and Terms

- None

Administration of this Standard

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

- **Reporting.** It is important that you immediately report any suspected violation of this Standard by a Catalyst employee or third party to your manager or to HR. All good faith allegations of violations of this Standard will be fully and confidentially investigated.

- **Exception to Standard.** Limited exceptions to the Standard may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Standard. Any request for an exception to the requirements of this Standard must be submitted to the Information Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.

- **Applicability.** This Standard 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
06/17/2020	James Mbassa	Initial release.	Owner