CATALYST
WORKPLACES THAT WORK FOR WOMEN

INFORMATION SECURITY PROGRAM

Effective: September 1, 2020

Information is one of Catalyst's most valuable assets. In order to maintain and establish trust between Catalyst and its Supporters, the protection of information is critical. Catalyst would suffer an adverse impact if information vital to fulfill its mission was no longer available, became altered or distorted, or was received by unauthorized users.

Purpose of Program

While Catalyst encourages flexibility in how and where work is done, the security of its data is a core element of its philosophy. This Program, and its supporting policies and standards, have been formulated in order to provide staff with a clear understanding of their responsibility toward protecting informational assets.

Catalyst is committed to fully complying with applicable laws, internationally accepted principles and requirements for data protection wherever we do business. This is vital to our continued success in an increasingly regulated global marketplace and reflects our commitment to conduct business in accordance with the highest legal and ethical standards.

As a U.S. based organization with operations worldwide, including within the European Union, Catalyst is subject to regulations under the laws of the United States, the Member States of the European Union, Canada, and various other countries covering the information we process concerning our members, business partners, and employees. This Program is intended to help users understand our data practices in place to comply with these laws and regulations. At Catalyst, we require full compliance with this Program to help ensure adherence to applicable data privacy and security laws.

Application of Program

This Program applies to all systems storing, processing or transmitting information owned, controlled, or managed by Catalyst. This Program applies to all Catalyst employees, contractors, vendors and agents with access to Catalyst information.

Catalyst is committed to complying with the applicable data privacy and security requirements in the countries in which it operates. Because of differences among these jurisdictions, Catalyst has adopted this Program to create a common core of values, policies and procedures intended to achieve nearly universal compliance, supplemented with alternative or additional policies or implementation procedures applicable in those jurisdictions with unique requirements.

This Program follows internationally accepted principles of data protection, without superseding the requirements of existing national laws. It applies in all cases as far as it is not in conflict with the respective national law; additionally, the national law in specific countries shall apply if it makes greater demands. National law applies in the case that it entails a mandatory deviation from or exceeds the scope of this Policy for data protection. This Policy also applies in countries in which there is no corresponding national legislation in place.

Program

Catalyst maintains a suite of relevant security-related policies and procedures. Updates to these policies and procedures are performed on at least a yearly basis. The list of policies are as follows:

Policy/Standard Name	General Purpose
Anti-Malware	Describes solutions intended to ensure that Catalyst can prevent malicious software while effectively and efficiently achieving its business objectives and conducting business.
Cloud Vendor Management	This Standard is intended to ensure that all of Catalyst's legal, ethical and standard compliance requirements are met in the procurement, evaluation and use of cloud services.
Information Governance/ **Data Classification**	Establishes the principles of information governance for the identification, classification, protection, retention and disposition of Catalyst information to meet Catalyst's legal, regulatory and business operational requirements.
Internet Use Monitoring and Filtering	Defines standards for systems that monitor and limit web use from any host within or accessing Catalyst's network.
Log Monitoring	Specifies requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.
Network Security	Defines the precautions designed to safeguard Catalyst's systems, networks and data.
Password Standard	Defines a standard for the creation of strong passwords, protection of those passwords and frequency of change.
Patch and Vulnerability Management	Describes the requirements for maintaining effective protection against internal and external attacks to protect Catalyst Information Technology resources that are susceptible to vulnerabilities and must have processes to prevent, detect and remediate in a timely manner to mitigate risk.
Physical Security	Establishes standards for securing access to Catalyst facilities.

Remote Access	Defines requirements for connecting to Catalyst's network from any host while remote to Catalyst facilities.
Reporting of Information Security Incidents and Violations	Provides direction for staff reporting of observed information security incidents.
Security Awareness Training	Describes an information security awareness training program to increase Users' awareness of their information security responsibilities in protecting the confidentiality, integrity, and availability of Catalyst Information Resources.
Segregation of Duties	Defines the activities which should be separated in order to achieve the objective of properly segregating conflicting duties.
Software Management	Defines the standards for the approval, deployment and management of Catalyst-installed software.
User Access Management	Describes how accounts and privileges should be used, approved, granted, audited and deprovisioned.
Data Subject Rights Requests Procedure	Describes how Catalyst personnel should respond to a data subject rights request
Record Retention and Disposition Standard	Specifies the manner in which necessary records and documents are retained and ensures that records no longer needed are discarded at the proper time.
Website Privacy Notice	Describes Catalyst's privacy responsibilities and practices with respect to users of the Internet website, applications, and electronic communications
Employee Privacy Policy	Describes Catalyst's privacy responsibilities and practices with respect to employees

Access Justification/Authorization Process

Access authorization procedures comply with the following standards:

- Catalyst has a process in place designed to limit access to data to only authorized personnel having a business need for such data.
- Each authorization is approved by appropriate Catalyst management. The authorization and manager approval is documented and retained.
- Catalyst has in place a process that will promptly remove all access for employees that leave the organization or change jobs within the organization and no longer need access.
- Re-verification of individuals that have access to systems that host Catalyst data is performed to verify that malicious, out-of-date, or unknown accounts do not exist.

Audit and Compliance

Catalyst performs various types of internal and third-party audits to validate compliance with applicable requirements, laws and regulations. Upon completion of each audit, a written report of the findings and recommendations is created and maintained in a secure central repository. In the event that a non-compliance, deficiency or other finding is discovered during the course of an audit, Catalyst promptly assesses, prioritizes, mitigates or identifies appropriate compensating controls.

Disaster Recovery

Data Recovery

Catalyst has the ability to recover data in the event of a disaster or for business continuity purposes. Catalyst maintains a Data Recovery Process, covering back-up and restore procedures.

Offsite Backups

Catalyst adheres to and maintains measures to secure data being transported offsite for usage, hosting, backup, and/or storage. This includes:

- Storing backups in a secure off-site facility
- Maintaining strict control over the distribution of any back-ups
- Transmission of data via secured protocols

Change Management

Changes to information resources are managed and executed according to a defined ticket and change management process. This process helps Catalyst review, authorize, test, document and implement/release in-scope proposed changes in a controlled manner, and monitor the status of each proposed change.

Data Disposal and Hardware Sanitization

Catalyst performs sanitization of media containing Catalyst data. Data is disposed of utilizing one of the following three methods:

- **Overwriting:** The software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data, rendering the data unrecoverable.
- **Degaussing:** Exposing the media to strong magnetic fields to destroy its contents. This method eliminates any data still on the media.
- **Physical Destruction:** This includes shredding or any other method of physical destruction including extremes of physical force and temperature. Physical destruction is accomplished in a manner that precludes further use of the media.

Data Loss Prevention

Catalyst has implemented a variety of processes and technologies to identify and manage data loss events across key Catalyst internal business applications, such as corporate email and sanctioned collaboration tools.

Encryption

Catalyst provides protection of data through a combination of access controls and encryption. Encryption is required if:

- Data is transmitted over public or wireless networks.
- Catalyst determines that encryption at rest is necessary to protect data.

Incident Response

Catalyst maintains an Incident Response Plan, which details procedures to be followed in the event of an actual or reasonably suspected unauthorized access to or use of Catalyst data, including but not limited to disclosure, theft or manipulation of data that has the potential to cause harm to Catalyst systems, data, or the Catalyst brand name.

Risk Assessment and Penetration Testing

Catalyst conducts regular third-party risk assessments and penetration tests on applications, systems, and infrastructure associated with accessing, processing, storage, communication and/or transmission of sensitive data.

Privacy

Catalyst is committed to complying with data privacy laws. It has implemented numerous technical and administrative measures for the protection and security of data.

Vendor Management

Catalyst has developed and implemented a program to evaluate relevant third-party vendors and partners prior to engaging in a business relationship and regularly thereafter. Catalyst’s vendor management program takes a risk-based approach to evaluate the security maturity, compliance and functionality available.

Information Security Officer (ISO) Responsibilities

Catalyst's ISO (VP, Information Technology) is responsible for initiating and reviewing the implementation of this policy. The ISO and Chief Privacy Officer, working in conjunction with other departments within Catalyst will develop and maintain required policies, procedures and standards that are necessary to ensure data security. They will administer and monitor security controls appropriate for Catalyst, including but not limited to:

- Access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to ensure the principle of least privilege.
- Access restrictions at physical locations containing information, such as buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals.

- Encryption of electronic information whenever possible, including while in transit or storage on networks or systems to which unauthorized individuals may have access.
- Monitoring systems to detect actual and attempted intrusions into information systems.
- Response programs that specify actions to be taken when Catalyst suspects or detects that unauthorized individuals have gained access to information systems, including appropriate reports to regulatory and law enforcement agencies.
- Measures to protect against the destruction, loss, or damage of information due to potential environmental hazards or technological failures.

- Publish guidelines that apply to specific jurisdictions to the extent such jurisdictions require a deviation from this Program.

Catalyst's ISO will be the primary source of contact regarding information security considerations related to technical, environmental, or regulatory changes that may arise in the future.

Administration of this Policy

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

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

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

- **Applicability.** This program 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.

- **Proportionality.** Catalyst will apply this Program in a reasonable manner, with cost and effort proportionate to the importance of the proposed personal data processing and the sensitivity of the data at issue.

- **Effect of Program.** This Program shall not be interpreted or construed as giving any individual rights greater than those that such person would be entitled to under applicable law and other binding agreements with Catalyst.

Revision History

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