INCIDENT RESPONSE PLAN

Effective: September 1, 2020

Purpose of Plan

This Plan is intended to provide a structured and systematic incident response process for all information security incidents (as hereinafter defined) that affect any of Catalyst's information technology ("IT") systems, network, or data. This Plan will define to whom the incident response process applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, as well as reporting, remediation, and feedback mechanisms. This Plan is designed to assist Catalyst and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents, mitigating or minimizing the effects of any information security incident, and engaging stakeholders and driving appropriate participation in resolving information security incidents while fostering continuous improvement in Catalyst's information security program and incident response process.

Application of Plan

This Plan applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Catalyst data. Catalyst may, from time to time, approve and make available more detailed or location or work group-specific plans, policies, procedures, standards, or processes to address specific information security issues or incident response procedures. Those additional plans, policies, procedures, standards, and processes are extensions to this Plan.

Catalyst has designated James Mbassa, VP, Information Technology to implement and maintain this Plan.

Information security is a priority at Catalyst. We take the security of our people and our information very seriously. We strive to avoid and prevent data security incidents, but if one does occur, it is important to promptly respond in accordance with this policy to avoid harm to Catalyst and its employees, members, vendors, and supporters.

All members of the Catalyst community are responsible for reporting known or suspected information or information technology security Incidents. All Incidents at Company must be promptly reported as set forth in this Plan

Incident Response Team

The Incident Response Team ("IRT") is responsible for managing Incidents involving the loss or unauthorized access of personal data and personal information and other security incidents involving Catalyst data or network systems. The IRT will keep abreast of relevant threats, vulnerabilities or alerts from actual incidents. The IRT has authority to make decisions related to the incident and to make required notifications. The IRT consists of:

Role	Name	Email	Cell Phone
CFAO	Stacey Bain	sbain@catalyst.org	973 723 9477
VP, Global Admin & Legal Affairs, and Chief Privacy Officer	Emily Zuckerman	ezuckerman@catalyst.org	646 391 8187
VP, Information Technology	James Mbassa	jmbassa@catalyst.org	917 531 3677
Senior Director, Digital	Jeanne McCabe	jmccabe@catalyst.org	917 482 5416
Vice President Human Resources	Jennifer Potthoff	jpotthoff@catalyst.org	412 519 7209
Senior Director, Internal Communications	Doug Novarro	dnovarro@catalyst.org	516 521 0239
VP, Media & Public Relations	Naomi Patton	npatton@catalyst.org	917 359 6464
Director, Office Management	Meredith Lanham	mlanham@catalyst.org	270 704 2805
Senior Associate	Fabienne Parsons	fparsons@catalyst.org	647 624 3750

Through this Plan, Catalyst authorizes the IRT to take reasonable and appropriate steps necessary to mitigate and resolve information security incidents, in accordance with the escalation and notification procedures defined in this Plan. The IRT is responsible for:

- Addressing information security incidents in a timely manner, according to this Plan.
- Managing internal and external communications regarding Incidents.
- Reporting its findings to management and to applicable authorities, as appropriate.
- Reprioritizing other work responsibilities to permit a timely response to Incidents on notification.

Note: Specific responsibilities set forth in this Plan are listed to distribute tasks and help prevent important actions from being overlooked; however, all team members should be prepared to assist any other team member with any action as required or in the best interest of Catalyst.

Note: Although the steps set forth in this Plan should be applied to any and every Incident, the actual scope of the investigation and response will depend on the type and severity of the Incident. For example, an Incident involving personal data will require a more thorough investigation and response than an Incident that does not involve such data.

Plan

1. **Discovery and Reporting:**

    a. Any individual who suspects that a theft, breach or unauthorized exposure or access of Catalyst data or Catalyst IT systems (an “Incident”) has occurred must immediately provide a description of what occurred via e-mail to it@catalyst.org, by calling Catalyst’s IT consultants, CMIT, at 1-866-520-6414, or through the use of the Help Desk chat tool. These communication channels are monitored by Catalyst’s IT Department. Incidents or potential Incidents should be reported immediately upon discovery, but in no event later than 24 hours after discovery.

    b. As soon as an Incident is identified, the CFAO will chair the IRT to handle the event. The IRT shall review the details of the report and prepare for the investigation, if warranted. The CFAO, VP, Global Admin & Legal Affairs and Chief Privacy Officer, VP, Information

Technology, and Senior Director, Internal Communications will be involved in all Incident responses and investigations. The Senior Director, Digital will be a part of the IRT if the incident is web-related. The Vice President Human Resources will be a part of the IRT if the incident involves employee data or an employee actor. The VP, Media & Public Relations will be part of the IRT if it is determined that external communications will be required. The Director, Office Management and the Senior Associate, Toronto Office will be part of the IRT if the incident implicates on-premises facilities.

c. The key during this stage is to ensure that Incidents are identified and that the proper parties are made aware of Incidents so that Catalyst can respond to any such incident in a prompt, orderly manner.

d. Catalyst shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. Catalyst shall document each identified Incident.

e. Following identification of an Incident, the CFAO, or a designate, shall perform an initial risk-based assessment and determine the level of response required based on the Incident's characteristics, including affected systems and data, and potential risks and impact to Catalyst and its supporters, employees, or others.

2. **Investigation:**

a. Once an Incident is reported to a member of the IRT, the IRT members will coordinate to begin the response in accordance with this Plan. This step is critical because the information obtained and the steps taken immediately after discovery can impact the investigation and ensuing response.

b. At the direction of the VP, Global Admin & Legal Affairs and Chief Privacy Officer, the IT Department, along with a designated forensic team, will analyze the breach or exposure to determine how the breach or exposure occurred, the types of data involved, and the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause. The IT Department and forensic team also shall determine how best to collect and preserve evidence. This investigation should be performed in an expedient manner, with closure commensurate with the nature of the breach. The IT Department and forensic team shall provide constant updates to the other members of the IRT. All other communications regarding the Incident shall be at the direction of the VP, Global Admin & Legal Affairs and Chief Privacy Officer.

c. The VP, Global Admin & Legal Affairs and Chief Privacy Officer shall determine whether to contact external legal Incident counsel.

d. The VP, Global Admin & Legal Affairs and Chief Privacy Officer shall determine whether to notify Catalyst leadership and any applicable business partners or service providers, Catalyst's insurance carrier, and law enforcement or other authorities.

e. The IRT shall document its investigation and analysis for each identified Incident under the direction of the VP, Global Admin & Legal Affairs and Chief Privacy Officer.

f. Note: Some vendors, including credit card companies, have specific evidence preservation procedures that must be followed.

3. **Containment and Remediation:**

   a. Under the direction of the IT Department and forensic team the affected host or system will be identified, isolated or otherwise mitigated. After the repair of affected systems, an analysis will be performed to confirm the threat has been contained prior to bringing affected systems back online.

   b. The IRT shall direct appropriate internal or external resources to capture and preserve evidence related to each identified Incident during investigation, analysis, and response activities. The IRT shall seek counsel's advice, as needed, to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific information security incidents.

4. **Communication and Notifications:**

   a. All information regarding a breach should be treated as confidential information. Catalyst's CFAO and Communications and Legal Departments will determine decide how to communicate the breach to a) internal employees, b) Supporters, c) the public, and d) those directly affected. Only the IRT may authorize Incident-related communications or notifications. The IRT shall seek counsel's advice, as needed, to review communications and notifications targets, content, and protocols.

   b. Under the direction of the VP, Media & Public Relations, the IRT shall prepare and distribute any external communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

   c. The IRT shall report criminal activity or threats to applicable authorities, as Catalyst deems appropriate under the guidance of counsel.

   d. While the IRT may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require Catalyst to notify various parties of some information security incidents. The VP, Global Admin & Legal Affairs and Chief Privacy Officer and external incident counsel shall determine the timing and content of any such required notices.

5. **Post-Incident Activity:**
   a. In addition to creating a follow-up report for each incident, Catalyst will hold a "lessons learned" meeting after every major security incident, and optionally after lesser incidents if appropriate. Questions to be answered in "lessons learned" meetings include:
      i. Exactly what happened, and at what times?
      ii. What vendors were involved and what recommendations did they make?
      iii. What root cause was provided by the impacted vendors?
      iv. How well did staff and management perform in dealing with the incident?

v. Were documented procedures followed, and were they adequate?
vi. What information was needed sooner?
vii. Were any steps or actions taken that might have delayed or inhibited the recovery?
viii. What would the staff and management do differently the next time a similar incident occurs?
ix. What corrective actions can prevent future-like incidents?
x. What precursors or indicators should be watched for in the future to detect similar incidents?
xi. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
xii. What changes, if any, should be made to this Plan?

b. The CFAO shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including communicating its recommendations to and seeking necessary authorization or support from Catalyst leadership.

Plan Training and Testing

- **Training.** The CFAO shall develop, maintain, and deliver training regarding this Plan periodically.

- **Testing.** The CFAO shall coordinate exercises to test this Plan periodically. The CFAO shall document test results, lessons learned, and feedback and address them in Plan reviews.

- **Plan Review.** Catalyst shall review this Plan at least annually, or whenever there is a material change in Catalyst's business practices that may reasonably affect the response procedures. Plan reviews will also include feedback collected from post-incident reviews and training and testing exercises. The CFAO must approve any changes to this Plan and is responsible for communicating changes to affected parties.

Related Standards, Policies and Processes

- Catalyst's Employee Handbook

Definitions and Terms

- Capitalized terms defined as set forth herein.

Administration of this Plan

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

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

- **Exception to Plan.** Limited exceptions to the Plan may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Plan. Any request for an exception to the requirements of this Plan must be submitted to the Information

Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.

- **Applicability.** This Plan 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.

- **Enforcement**. Violations of or actions contrary to this Plan may result in disciplinary action, in accordance with Catalyst's information security policies and procedures and human resources policies. Please see Catalyst's Employee Handbook for details regarding Catalyst's disciplinary process.

Revision History

Date	Name	Description	Responsibility
09/1/2020	James Mbassa	Initial release.	Owner