REPORTING OF INFORMATION SECURITY INCIDENTS AND VIOLATIONS STANDARD

Effective: September 1, 2020

Purpose of Standard

The purpose of this Standard is to provide direction for user reporting of Information Security Incidents. An Information Security Incident is an event that affects the security, availability, confidentiality or integrity of Catalyst's information technology network or the data residing therein, including an event with potential impact to Catalyst, Supporter, or employee personal information or intellectual property, or impact to other information that could result in damage to Catalyst's assets or reputation.

Application of Standard

This Standard applies to all Catalyst employees, contractors and vendors.

Standard

The following information security standards shall be implemented and actively enforced to minimize the damage from Information Security Incidents:

1. Immediately report any suspected or observed information security incidents including, but not limited to:
    a. Virus / Malware
    b. Suspected Phishing / Scam
    c. Information security breach
    d. Password misuse
    e. Suspicious / Inappropriate handling of Catalyst's data
    f. Denial of service
    g. Suspected server / workstation compromise
    h. Malicious Internal / External intrusion attempt
2. Report any Information Security Incident immediately through one of the following channels:
    a. secure@catalyst.org

b. 1-866-520-6414

3. Chief Privacy Officer will report identified breaches to the applicable authority whenever required by law.

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

- None

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
09/01/2020	James Mbassa	Initial release.	Owner