SECURITY AWARENESS TRAINING POLICY

Effective: September 1, 2020

Purpose of Policy

This policy is intended to ensure that security awareness training is conducted for all employees with the goal of better protecting Catalyst's confidentiality, integrity, and availability of its information resources and data.

Application of Policy

This Policy applies to all Information Systems and Information Resources owned or operated by or on behalf of Catalyst. All persons with access to Catalyst information or computers and systems operated or maintained on behalf of Catalyst are responsible for adhering to this Policy.

Policy

The VP, Information Technology and the Human Resources Department shall define and implement 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. Annually, a skills gap analysis will be performed to understand the skills and behaviors employees are not adhering to, and use this information to build a baseline education roadmap. Training will be delivered to address the skills gap identified to positively impact the employee's security behavior.

Security Awareness Training

All employees with access to Catalyst Information Resources must complete security awareness training within the first 30 days from date of hire. Information Security Refresher Training must be completed annually. Catalyst's security awareness program is updated at least annually to address new technologies, threats, standards, and business requirements. Employees will be trained on:

- The importance of enabling and utilizing secure authentication;
- How to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls;
- How to identify and properly store, transfer, archive, and destroy sensitive information;
- How to identify the most common indicators of an incident and be able to report such an incident.

At least quarterly, newsletters or other training aids will be distributed to all staff to reinforce security awareness.

Role-Based Security Awareness Training

The extent of security-related training shall reflect the person's individual responsibility for using, configuring, and/or maintaining information systems. Training shall be provided to users and technical staff in critical areas of cybersecurity, including vendor-specific recommended safeguards.

- Role-based security-related training shall be provided before authorizing a person's access to a system; before they are allowed to perform their assigned duties; and when required by system changes.
- Training in cybersecurity threats and safeguards, with the technical details to reflect the staff's individual responsibility for configuring and maintaining information security is required.
- Annual re-occurring training shall be provided thereafter.
- Additional education for information security professionals and jobs requiring expertise in security will be provided as needed through formal external courses and certification programs.

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

- None

Definitions and Terms

- None

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