PHYSICAL SECURITY POLICY

Effective: September 1, 2020

Technology can address many threats, but physical security measures are also required to address any non-technical threats to information, equipment, and the infrastructure.

Purpose of Policy

This Policy is intended to establish standards for securing access to Catalyst offices, data centers, network closets and Information Technology (IT) facilities. Effective implementation of this Policy will minimize unauthorized access to these locations and provide more effective auditing of physical access controls.

Application of Policy

This Policy applies to all Catalyst owned or operated facilities.

Technical Requirements

- Physical access to all facilities or locations must be documented and managed.
- Effective lighting and sufficient fire alarms and sprinklers must be installed.
- All IT facilities must be physically protected in proportion to the criticality or importance of their function.
- Access to IT facilities will be granted only to the Catalyst personnel and contractors whose job responsibilities require access to that facility.
- The process for granting card and/or key access to IT facilities must include approval from the Information Technology department.
- Access cards and/or keys must not be shared or loaned to others, and those that are no longer needed must be returned.
- Lost or stolen access cards and/or keys must be reported within 24 hours.
- Card access records and keys logs for IT facilities must be kept for routine review based upon the criticality of the resources being protected.
- Visitors must be escorted in access-controlled areas.

- IT must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, but minimally discernible evidence of the importance of the location should be displayed.

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 Policy.** 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