CATALYST
WORKPLACES THAT WORK FOR WOMEN

SOFTWARE MANAGEMENT STANDARD

Effective: September 1, 2020

Allowing employees to install software on Catalyst-owned computing devices exposes the organization to unnecessary risk. Installing unauthorized software can introduce conflicting file versions or DLLs which prevent programs from running, malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can compromise the organization's network.

Purpose of Standard

The purpose of this Standard is to reduce compliance and security risks and control IT expense. This document defines the standards of Catalyst software management. This Standard will minimize the risk of loss of program functionality, the exposure of sensitive information from Catalyst's computing network, the risk of introducing malware and the legal exposure of violating vendor contracts and copyright laws.

Application of Standard

This Standard applies to all Catalyst employees, contractors, vendors and agents with Catalyst-owned devices. This Standard covers all computers, servers, smartphones, tablets and other computing devices operating within Catalyst.

Standard

1. All software shall be acquired through channels approved by following the Purchasing Policy.
2. Only Catalyst-approved software will be installed and supported by Catalyst IT or persons authorized and under the direction of Catalyst IT.
3. Catalyst does not support employee-owned software on Catalyst-owned assets.
4. Employees may not install software on Catalyst-owned computing devices.
5. Requests to install software must be submitted by the employee's manager, in writing, to the IT Department's Help Desk.
6. It is a violation of this Standard to disable any asset-tracking, anti-malware or systems management software installed on a Catalyst system.

7. The IT Department will conduct periodic software audits of Catalyst-owned assets to ensure compliance with security standards and vendor contracts.

8. Catalyst IT will report and remove unauthorized software detected on corporate-owned assets.

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