Anti-Malware Standard

Effective: September 1, 2020

Purpose of Standard

The purpose of this Standard is to ensure that Catalyst can stop malicious software while effectively and efficiently achieving its business objectives and conducting business. The goal is to ensure that:

- Activity stemming from malicious software (Viruses, Trojans, Worms, Spyware, etc.) is prevented or mitigated.
- Unauthorized access to Catalyst resources and information via malicious software is prevented or mitigated.
- Availability of Catalyst's computer resources is not severely impacted by an introduced piece of malicious software.

Application of Standard

This Standard applies to:

1. Catalyst systems that can contain applications and data vulnerable to infections.
2. Any system deployed to run Catalyst corporate business operations.
3. Systems or system images provided, managed and/or supported by the Catalyst Information Technology (IT) Department.
4. Any system or device used by Catalyst employees and contractors to access Catalyst systems and data.

Standard

1. The Catalyst-defined standard anti-malware solution must be installed on all servers, desktops and notebooks and must remain operational and adherent to configuration settings supplied by the IT Department.
2. The Catalyst-defined standard threat logging and monitoring solution must be installed on all servers, desktops and notebooks and must remain operational and adhere configuration settings supplied by the IT Department.

3. The Catalyst-defined standard Host Intrusion Prevention (HIPS) solution must be installed on all desktops and notebooks and must remain operational and adhere to configuration settings supplied by the IT Department.

4. The Catalyst-defined standard client firewall solution must be installed on all servers, desktops and notebooks and must remain operational and adhere to configuration settings supplied by the IT Department.

5. The Catalyst-defined standard endpoint encryption solution must be installed on all desktops and notebooks and must remain operational and adhere to configuration settings supplied by the IT Department.

6. Network-attached storage must have applicable content scanned by the Catalyst-defined standard anti-malware solution during file read, write or execute.

    a. Removable media such as USB and DVD-ROM will be disabled and generally not permitted to be connected to Catalyst laptops.

7. Web traffic processed by Catalyst IT firewalls must be scanned with an anti-malware solution.

8. Email traffic processed by Catalyst IT must be scanned with an anti-malware solution.

9. Catalyst employees and contractors will be required to make their managed systems available for routine patching and updates.

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