PATCH AND VULNERABILITY MANAGEMENT STANDARD

Effective: September 1, 2020

Catalyst is responsible for ensuring the confidentiality, integrity, and availability of its data and that of client and Supporter data stored on its systems. Catalyst has an obligation to provide appropriate protection against threats which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this Standard will limit the exposure and effect of common attack vectors to the systems within this scope.

Purpose of Standard

This Standard describes the requirements for maintaining effective protection against internal and external attacks to protect applications and systems managed by Catalyst ("Catalyst Information Technology resources").

Application of Standard

This Standard applies to Catalyst Information Technology resources, regardless of location, that are susceptible to vulnerabilities and must have processes to prevent, detect and remediate in a timely manner to mitigate risk.

Standard

Patching:

1. Security patches that affect Catalyst's Information Technology resources must be rated as to risk, and deployed within timeframes appropriate to their rated risk.
    a. Patches for critical and high-security vulnerabilities must be installed within 14 days of release on High-Value Assets.
    b. Patches for medium and low-security vulnerabilities must be installed within 90 days of release.
2. Exceptions to patching must be documented with a planned remediation date and acceptance of risk by the ISO if non-compliance poses a critical threat to the Catalyst network or compliance requirements.

Vulnerability Management:

1. Only current and vendor-support OSes and software may be deployed. All deviations require a documented migration plan and risk mitigation strategy.
2. All Catalyst systems must be scanned on a periodic basis. The frequency of these scans will depend on the asset type, criticality and exposure.
    a. For High-Value Assets, vulnerability scans must run at a minimum on a monthly basis.
    b. For other assets, vulnerability scans must run at a minimum on a quarterly basis.
3. Vulnerability remediation efforts for critical vulnerabilities and High-Value Assets must be tracked and monitored.
4. Vulnerability remediation must be verified by subsequent scans.

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

- **High-Value Assets**. Publicly accessible network infrastructure and critical systems.

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