REMOTE ACCESS STANDARD

Effective: September 1, 2020

Purpose of Standard

Remote access to the Catalyst corporate network is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than Catalyst's corporate network. While these remote networks are beyond the control of this Standard, Catalyst must mitigate these external risks the best of its ability.

This Standard is intended to define rules and requirements for connecting to Catalyst's network from any host. These rules and requirements are designed to minimize the potential exposure to Catalyst from damages which may result from unauthorized use of Catalyst resources. Damages include the loss of sensitive or company confidential data or intellectual property, damage to Catalyst's reputation, damage to critical Catalyst internal systems, and fines or other financial liabilities incurred as a result of those losses.

Application of Standard

This Standard applies to all Catalyst employees, contractors, vendors and agents permitted to connect to the Catalyst network while remote to Catalyst facilities. This Standard covers any and all technical implementations of remote access used to connect to Catalyst networks. Only assets managed by Catalyst shall be permitted full remote access into the Catalyst network. Unmanaged assets shall only have limited access to the Catalyst environment.

Standard

The following remote access security standards shall be implemented and actively enforced:

1. **Authorization:** Authorization for remote access to the Catalyst network shall be:

    a. Managed: Remote access solutions shall include a procedure for requesting, granting, and monitoring access granted to remote users.

    b. Logged: Successful and failed connection attempts will be logged and collected in a central repository for review. The minimum information required to be logged are time, source IP address, and username.

    c. Audited: Remote access solutions shall include the ability to periodically review and audit access. In the absence of automated correlation techniques, manual audits will be performed monthly.

2. **Authentication:** Client credentials presented to Catalyst systems for purposes of establishing remote access shall be:

    a. Multifactor: Authentication using Catalyst Windows credentials shall serve as first factor, and a token or certificate shall serve as the second factor. Trusted source IPs belonging to certified solution providers may serve as second factor when tokens or certificates are not feasible.

    b. Encrypted: Client credentials supplied for the purposes of establishing a remote connection to Catalyst resources shall use an encryption method based on cryptographic techniques that provide strong authentication and security.

    c. Trusted: Client credentials furnished for purposes of gaining remote access to Catalyst systems shall be authenticated using a known, trustworthy security principle that is managed by Catalyst IT.

    d. Revocable: Client remote access privileges shall be revocable at any time.

3. **Encryption:** Network traffic between the devices and the Catalyst network shall use an encryption method based on cryptographic techniques that provide strong authentication and security.

4. **Software:** Only software approved and supported by Catalyst IT shall be used for remote access to the Catalyst network.

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

- Internet Use Monitoring and Filtering Standard
- Log Monitoring Standard

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