CATALYST

WORKPLACES THAT WORK FOR WOMEN

PASSWORD STANDARD

Effective: September 1, 2020

Passwords are an important aspect of computer security. A poorly-chosen password may result in unauthorized access and/or exploitation of Catalyst's resources. All users, including contractors and vendors with access to Catalyst systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose of Standard

The purpose of this Standard is to establish a standard for creation and protection of strong passwords.

Application of Standard

The scope of this Standard includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Catalyst facility, has access to the Catalyst network, or stores any non-public Catalyst information.

Standard

1. General Password Protection

a. Do not reuse passwords. Don't use a password that is the same or similar to one you use on any other system.

b. Only enter passwords when using a known and trusted device.

c. Don't use a single word, for example, password, or a commonly-used phrase like Iloveyou.

d. Make passwords hard to guess, even by those who know a lot about you, such as the names and birthdays of your friends and family, your favorite bands, and phrases you like to use.

e. Passwords must never be written down.

f. Never reveal your passwords. If a password is revealed, change it immediately.

g. Do not hint at the format of a password (for example, "my family name").

2. Password Construction

a. Passwords must be a minimum of 8 characters in length.

b. Administrative or privileged accounts passwords must be a minimum of 15 characters.

c. Passwords must contain characters from the following categories:

    i. Uppercase characters (A through Z)

    ii. Lowercase characters (a through z)

    iii. Numeric digits (0 through 9)

3. Password Lifecycle

a. Passwords must be changed on first login and after administrative password resets (excluding service accounts).

b. Any default passwords must be changed upon system implementation.

c. Accounts must lock after six (6) consecutive incorrect password attempts. The account may be unlocked automatically after 30 minutes or manually by an administrator.

d. Any user suspecting that his/her password may have been compromised must report the incident and change the password.

4. Technical Requirements

a. Passwords are to be used in conjunction with multi-factor authentication (MFA) whenever technically feasible.

b. Passwords and User IDs must not be transmitted within the same electronic media (e.g., email) unless the message is encrypted.

c. Users must not hard code any passwords in scripts or clear text files such as shell scripts, batch jobs or word processing documents.

d. Application and/or web developers must ensure that their programs contain the following security precautions:

    i. Applications must support authentication of individual users.

    ii. Applications must not store passwords in clear text or in any easily reversible form.

    iii. Applications must not transmit passwords in clear text over the network.

    iv. Applications must provide for role management, such that one user can take over the functions of another without having to know the other user's password.

    v. Applications should use token based modern authentication methodologies. Legacy insecure authentication protocols should not be used.

  e. Privileged (administrative) access must use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not for internet browsing, email, or similar activities.

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

- **Multi-factor authentication:** A security system that verifies a user's identity by requiring multiple credentials. Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification).

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