CATALYST
WORKPLACES THAT WORK FOR WOMEN

# USER ACCESS MANAGEMENT STANDARD

**Effective:** September 1, 2020

Protecting access to Information Technology (IT) systems and applications is critical to maintain the integrity of Catalyst technology and data and to prevent unauthorized access to such resources. Access to Catalyst systems must be restricted to only authorized users or processes, based on a need-to-know basis (the principle of “Need to Know”), and with the least amount of access privilege granted as needed (the principle of “Least Privilege”). Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job-related duties.

## Purpose of Standard

This Standard is intended to describe how accounts and privileges should be used, approved, granted, audited and deprovisioned.

## Application of Standard

This Standard applies to all users of Catalyst shared information, systems and services, in addition to those responsible for the management of the same.

## Standard

1. Access Requirements

    a. Users must have an established identity in a trusted store.

    b. Users must use privileges associated with an account only for the purpose for which they were authorized and no more (following the principle of Least Privilege).

    c. Users must use privileged accounts and authorizations only when such privilege is needed to complete a function.

    d. All access must have an auditable trail of request, approval, creation, modification and removal.

    e. Individual accounts must not be used by anyone other than the account owner.

    f. Passwords must meet the minimum requirements when they are created, changed or handled as specified in the *Password Standard*.

   g. Access to systems and software granted by Catalyst should only be used for Catalyst's legitimate purposes and should not be used for personal, unethical or illegal activities.

2. Access Request and Approvals: All requests for authorization must be approved by an administrative and technical approver. These approvers must be two (2) different people to ensure segregation of duties.

   a. Administrative Approval: The administrative approval confirms that the authorization requested is needed to perform a required function. The approver should sufficiently understand the full scope of the authorization being granted before making a decision and ensure Least Privilege is applied.

   b. Technical Approval: The technical approval confirms that the privilege requested is required to achieve the approved administrative need. The approver should sufficiently understand the full scope of the authorization being granted before making a decision and ensure Least Privilege is applied.

3. Access Provisioning: Before granting access to a system or application, the following must be adhered to:

   a. Role-based or "security group" authorization schemes shall be used rather than individual authorizations whenever practical.

   b. The ability to change permissions shall be restricted to the IT Department.

   c. Requests for access to data shall be approved by the business owner.

   d. Access obtained outside of the documented access request process must be reported and remediated accordingly.

4. Access reviews: The IT Department will perform reviews of Catalyst systems. These audits will ensure that accounts and authorizations are consistent with this document, including that:

   e. There is a request for every account;

   f. The request was approved both by an administrative and technical manager;

   g. The granted privileges were required for the approved use;

   h. Requests for temporary privileges are expired on the agreed expiration date;

   i. Every account is held by a person still employed or contracted to work for Catalyst;

   j. The account holder's job function still requires the granted privilege.

5. Deprovisioning

   a. Accounts listed in Active Directory will be disabled within one business day of user termination from Catalyst.

   b. If an account must remain active, it must be pre-approved by HR and Legal for a duration not to exceed 30 days past the termination date.

c. If the user had access to any shared accounts, the account owner must ensure that these accounts passwords are changed with 48 hours.

d. Passwords must be reset if the account is reactivated.

e. Accounts of terminated users will be deleted within 90 days unless required by legal, regulatory or compliance reasons.

6. Transfers

a. For users who transfer to another department or function and no longer require access, removal must be completed within 30 days.

b. If access in the new position violates segregation of duties access from the prior position, removal must be performed within 48 hours unless an exception is pre-approved by HR and Legal.

7. Extended Absences: Access not required during an extended absence from work must be temporarily disabled.

8. Access Types

a. Privileged Access

i. Privileged accounts must be owned by an individual Catalyst user.

ii. Privileged accounts must be kept to a minimum, individually approved, documented and strictly limited to those with a business justification for use.

iii. Privileged accounts must not be used for normal/general business use.

b. Third Party Access

i. Externally located vendors with access to the internal Catalyst network must have network restrictions in place.

ii. Vendors should not be given privileged or service account access unless specifically mandated in contract agreements for system and software maintenance purposes.

c. Temporary Access

i. Any access utilizing Temporary Accounts must be logged for audit purposes.

ii. Access to Temporary Accounts provided for emergency work must be disabled upon work completion and passwords must be reset at this time.

d. Service Accounts

i. Service accounts must not be accessed for personal use.

ii. All service accounts must have the Least Privilege it needs to run the service or process.

iii. Interactive logins to service accounts must be disabled to prevent direct login.

iv. Local Operating System service accounts are not permitted.

v. Service accounts have limited, specific use cases, and shall be deleted when no longer needed.

e. Default Accounts

i. Vendor-supplied default accounts credentials must be changed and unnecessary accounts removed before a platform or system is deployed in the Catalyst environment.

**Violations of Standard**

- **Non-Compliance.** An employee who violates this Policy may be subject to disciplinary action, up to and including termination of employment.

**Related Standards, Policies and Processes**

- Password Standard
- Segregation of Duties Standard

**Definitions and Terms**

- **Active Directory:** A Microsoft product that consists of several services to manage permissions and access to networked resources.
- **Trusted Store:** A system that stores and maintains user identities (e.g., Microsoft Active Directory).
- **Least Privilege:** A principle of granting only the minimum access necessary to perform an operation, and granting it only for the minimum amount of time necessary.

**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 |
|  |  |  |  |