| | | |
|---|---|---|
| | **Creation and Use of Authentication Mechanisms** | |
| | **Responsible Administrative Unit:**<br>Computing, Communications and Information Technology (CCIT) | **Policy Contact:**<br>Chief Information Security Officer<br>msendze@mines.edu |

## 1.0 BACKGROUND AND PURPOSE

This policy specifies that those accessing electronic services or resources belonging to Colorado School of Mines must use an authentication mechanism issued and maintained in accordance with best practice appropriate to the nature of the service or resource. The policy and its associated standards are intended to promote security, accountability and confidentiality in the assignment, maintenance and use of these personal credentials.

## 2.0 POLICY

Individuals wishing to access any electronic services or resources provided by Colorado School of Mines must first confirm their identity through an authentication mechanism. Commonly called login or sign-in, authentication mechanisms validate an individual's digital identity through the use of a personal identifier (most often a username) and one or more associated authenticators (passwords, phone codes, fingerprints etc.). Individuals are responsible for maintaining the confidentiality of all authenticators associated with their PID and are responsible for any access or activity taken using their identity.

## 3.0 Authentication and the Digital Identity Model

Colorado School of Mines uses an authentication framework based on the NIST Digital Identity Model described in Special Publication 800-63-3. The NIST model defines a Digital Identity as the unique representation of an individual accessing an electronic service or resource and authentication as the mechanism by which person demonstrates they are the individual associated with a Digital Identity.

Mines' authentication framework contains two components corresponding to these two aspects of the NIST model: the personal identifier used to associate a person with their digital identity and one or more authenticators used to demonstrate that the individual using a digital identity is in fact the person associated with that identity. A typical authentication process involves an individual presenting their personal identifier to the requested resource and then responding to one or more authentication challenges with the authenticator associated with their personal identifier.

### 3.1 Assignment and use of the Personal Identifier

Colorado School of Mines uses a personal identifier (PID), also known as a username or NetID, to represent the digital identity of students, faculty, staff, alumni, business partners and other affiliates of the university.

- One and only one PID is provided to an individual at the time the individual initially assumes or resumes a relationship with Mines. The PID remains the property of Colorado School of Mines who reserves the right to change, deleted, or add PIDs.
- Having a PID is a prerequisite for accessing electronic services however it does not in-and-of-itself authorize the use of any services or resources.
- Individuals may be assigned one or more secondary NetIDs associated with their PID. These secondary identifiers should be used only in authentication for the specific activities for which they were issued.
- The PID is also basic identifying information and, when used as an email identifier, is considered directory information consistent with Federal policy.

### 3.2 Authenticator(s)

An authenticator is something that an individual uses to respond to authentication challenges in order to authenticate their claim to a digital identity. Mines authentication framework recognizes three types of authenticators:

- Something one knows (i.e. a password).
- Something one has (i.e., an ID badge or cellular phone)
- Something one is (i.e., a fingerprint or other biometric data)

#### 3.2.1 Rules governing the use of knowledge-based authenticators.

Knowledge based authenticators are those authenticators which require an individual to demonstrate that they possess information that only they know. The most common knowledge-based authenticator is the password, but other types (e.g., passphrases, challenge questions) exist.

The unique nature of the password as an authenticator requires special attention. To help ensure the security of their authenticator, individuals are required to:

- Maintain the confidentiality of any knowledge-based authenticator at all times.
    - Passwords should never be shared with anyone at any time.
    - Passwords should never be stored or transmitted in an unencrypted format.
    - Passwords should be created with a degree of complexity that ensures their resistance dictionary attacks and to brute-force attempts using commonly available techniques.
- Passwords should be changed on a routine basis.
    - Unless multi-factor authentication is used passwords must be changed every six months.

- Each password must be unique.
    - Individuals creating passwords for multiple systems must generate different passwords for each system.
    - Passwords for different systems may not be based on a rubric or algorithm.

### 3.2.2 Rules governing the use of physical-based authenticators.

Physical-based authenticators are those authenticators which require an individual to demonstrate that they possess some physical device unique to their identity. Common physical-based authenticators include I.D. badges, cell phones, and one-time-password tokens.

- Individuals are welcome to use personally owned devices as authenticators, however Mines may not require an employee to provide or use a personal device.
    - This provision does not obligate Mines to provide a physical authenticator that is identical to those available to individuals who wish to purchase their own.
    - Individuals wishing to use personally owned devices must have the device vetted by the institution and recognize that Mines will collect personal information about the device.

### 3.2.3 Rules governing the use of biometric-based authenticators.

Biometric authenticators are those authenticators which rely on some characteristic of an individual's physical appearance or trait. Biometric authenticators include facial features, fingerprints or voice. Note that an individual's physical location may be considered a biometric authenticator.

### 3.3 Use of Multiple Authenticators

To improve the security of electronic resources and reduce the likelihood of a malicious actor could assuming an individual's digital identity individuals may use multiple authenticators when authenticating to a given resource. This process, known as Multi-Factor Authentication is current best practice. Its use is encouraged at all times and required for access to particularly sensitive systems.

- Additional factors must allow institutional access.
    - Individuals are required to use institutionally provided solutions if they are available for the resource being access.
    - If the individual is not utilizing a multi-factor solution provided by the institution they must provide the institution with a mechanism that allows access to the resource in their absence.
- Use two or more authentication factors.
    - When multi-factor authentication is used the lifetime of the primary credential may be extended or modified.

## 4.0 COMPLIANCE/ENFORCMENT

This policy issued by the Chief Information Security Officer under authority delegated to that office by the Board of Trustees. All members of Mines' community, including students, faculty, staff, alumni, business partners and other affiliates are required to comply with this policy. Enforcement of this policy is the responsibility of the office of Information Security who may take reasonable technical measures to address non-compliance or refer non-complaint individuals to the appropriate disciplinary mechanism.

## 5.0 EXCLUSION/DISCLAIMER (optional)

### 5.1 Service/System Accounts

Operating systems and automated processes make use of built-in accounts for accounting, Inter-Process Communication, management of automated processes and related system actives. As much as possible these accounts should be configured in a manner that prevents individuals from logging in or performing operations with these accounts. When that is not possible the authentication process used by these accounts must confirm to the standards described in section 3. When accessing resources with these account's there must be a mechanism to ensure the individual accessing the resources can be identified.

### 5.2 Vendor Accounts

Under rare circumstances Mines may assign a PID and associated credentials to a vendor or company rather than to an individual. When solution is utilized the Mines' employee managing the vendor relationship is required to ensure that the vendor agrees to:

- Maintain the ability to identify the individual making use of the credentials any time they are used.
- Notify Mines anytime an individual with knowledge of the credentials leaves the vendor or no longer needs access, at which time the primary credential must be changed.
- Ensure the privacy and security of the credentials, following all the standards described in section 3.

## 6.0 HISTORY AND REVIEW CYCLE

Published April, 2019. To be reviewed no less than annually.

## 7.0 DEFINITIONS

**Authentication** – A process by which an individual demonstrates that they are the individual associated with a given PID. Authentication is often confused with the process of verifying an individual's identity, known as **Identity Proofing**. For example; if an individual, John Doe, is assigned the PID *jdoe* with an associated password then

Identity Proofing would be the process John goes through to prove that he is in fact the real John Doe when he first contacts the school (this might be done with a government issued ID like a driver's license or by checking with trusted personal references). Authentication would be the process of providing that PID and password to a computer system in an attempt to demonstrate John is the person to which the jdoe PID was assigned.

**Authenticators** – An authenticator is something that an individual uses to respond to challenges in order to validate their claim to a digital identity. These are commonly referred to as "Something you know, Something you have, Something you are".

**Authorization** – A process by which an individual's authority to access a particular system or information is confirmed.

**Chief Information Security Officer** – The individual charged with coordinating efforts to ensure the confidentiality, integrity and availability of all campus electronic resources.

**Personal Identifier (PID)** – The token assigned to an individual that identifies associates their person with their digital identity. The most common example of a PID is a username, although the campus-wide ID and some cases an encryption key may also be used.

## 8.0 RESOURCES or ATTACHMENTS