# Identification and Authentication Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  | Signature: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage Identification and Authentication of the IT environment at [COMPANY NAME].

# Scope

This procedure is consistent with CMMC and covers all identification and authentication procedures within [COMPANY NAME] environment. This procedure will be followed by all employees of [COMPANY NAME].

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME]
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME].

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.5.1 - 3.5.11
* CMMC IA.L1-3.5.1- IA.L2-3.5.11
* [COMPANY NAME] – IA – 3.5 - Identification and Authentication Policy

# Procedure Statements

**IA.L1-3.5.1 – Identify information system users, processes acting on behalf of users or devices:**

1. The Information Systems uniquely identify company users which is centrally managed by Azure Active Directory and Azure Active Directory Domain Services. Identification and authentication is a two-part process wherein users present a unique identifier, commonly referred to as a User ID, to the Information System (identification) followed by an authenticator (password), which serves as proof/verification of the claimed identity (authentication).
2. The Information Systems uniquely identify processes and service accounts acting on behalf of company users, which is centrally managed by the Azure Active Directory and Azure Active Directory Domain Services. Information Systems require successful identification and authentication prior to access being granted. Established identifiers are unique to the individual to whom they are assigned, and group authenticators are not permitted for use on Information System components.

* Shared/Group accounts, other than the emergency administrator account, are not authorized for use on the Information Systems.

1. The System Administrator ensures that all Information System components are uniquely identified to being installed. Device identification is accomplished using the following:

* Identification: Each system possesses a unique MAC Address.
* Identification: Each system is assigned/possesses a unique IP Address.
* Identification: Each system is assigned/possesses a unique Hostname.

**IA.L1-3.5.2 - Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems:**

1. The Information Systems authenticate company users, or processes acting on behalf of company users, via the use of password authentication which is centrally managed by Azure Active Directory and Azure Active Directory Domain Services and Microsoft MFA. Identification and authentication is a two-part process wherein users present a unique identifier, commonly referred to as a User ID, to the Information System (identification) followed by an authenticator (password), which serves as proof/verification of the claimed identity (authentication).
2. The Information Systems uniquely identify processes and service accounts acting on behalf of company users, which is centrally managed by Azure Active Directory and Azure Active Directory Domain Services. Information Systems require successful identification and authentication prior to access being granted. Established identifiers are unique to the individual to whom they are assigned, and group authenticators are not permitted for use on Information System components.

* Shared/Group accounts, other than the emergency administrator account, are not authorized for use on the Information Systems.

1. Information System resources require successful identification and authentication prior to access being granted. Established identifiers (e.g., MAC address, Unique IP address, and Unique Hostname) are unique to the individual to whom they are assigned, and group authenticators are not permitted for use on Information System components.

* The identity of the individual, group, role, or device receiving the authenticator is verified as part of the initial authenticator distribution.
* Users are trained to never share their authenticators with anyone, including administrators.
* Lost, compromised, damaged, or unneeded authenticators are reported to the SA and the associated account is immediately disabled (revoking credentials).
* Default authenticators (e.g., default root/administrator passwords) that are shipped with systems and devices are changed prior to use.

**IA.L2-3.5.3 – Use of multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts:**

1. Privileged accounts are identified for local and network access by the <System Administrator>. The access control list detailing privileged accounts is maintained by the <System Administrator>.
2. [COMPANY NAME] employs multifactor authentication for local access on privileged accounts to organizational systems utilizing Azure Active Directory authentication methods to enforce Azure MFA. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks.

1. [COMPANY NAME] employs multifactor authentication for network access on privileged accounts to organizational systems utilizing Azure Active Directory authentication methods to enforce Azure MFA. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections.
2. [COMPANY NAME] employs multifactor authentication for network access on non-privileged accounts to organizational systems utilizing Microsoft Authenticator. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections.

* A combination of two factors for privileged and non-privileged accounts requiring local and network access include:
  + - * Something you know (Password and Personal Identification Number (PIN)).
      * Something you have (Token).

**IA.L2-3.5.4 - Replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts:**

1. The organizational information system implements Azure Active Directory authentication methods to enforce Azure MFA which incorporations replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts that are resilient to an adversary reusing captured information and gaining access to the computer resources.

* In order to protect against authentication replay attacks, several layers of authentication protection are in place on the information system, including:
  + Kerberos authentication protocol
  + TLS 1.2 encryption
  + Multifactor authentication
  + Nonce parameter used in authentication tokens
  + Low time-to-live (TTL) used in authentication tokens

**IA.L2-3.5.5 - Prevention of reuse of identifiers for a defined period:**

1. [COMPANY NAME] uses a unique user naming convention to ensure that identifiers are never reused, however when an [COMPANY NAME] information system user terminates, loses access to the system for cause, or no longer has a reason to access the [COMPANY NAME] information system, that individual's user identifier will be disabled. The period within which identifiers cannot be reused is as 12 months following reassignment or dismissal, once the user no longer requires access to the [COMPANY NAME] information system.
2. Recreation of a former staff members account during this period will not match the original identification. Accounts older than twelve (12) months are deleted with permission of the <role>. When a new account is being provisioned at [COMPANY NAME], the <role> and/or IT Department will review the deleted account records list to ensure identifiers are not reused. If the desired unique identifier is on the deleted account records list, then an alternative unique account identifier must be provisioned to ensure that the deleted account identifier is not reused.

**IA.L2-3.5.6** – **Disabling identifiers after a defined period of inactivity:**

1. The period of inactivity after which an identifier is disabled is set to 120 days.
2. Active identifiers are marked by the MSP, SecureStrux and disabled after 120 days of inactivity to avoid attackers from exploiting the inactive account

**IA.L2-3.5.7 - Enforcing a minimum password complexity and change of characters when new passwords are created:**

1. Password complexity requirements are defined:
   1. Minimum Password Length: 7 Characters
   2. Maximum Password Age: 90 Days
   3. Number of sign-ins before lockout: 5 attempts
   4. Password Complexity: Systems enforce a password complexity to include characters and amount of each from the following classes:
2. Uppercase characters
3. Lowercase characters
4. Numerical characters
5. Special characters
6. Password change of character requirements are defined to be 1 character between old and new passwords.

1. Minimum password complexity requirements as defined as above and are enforced when new passwords are created by using Azure Active Directory password protection GPOs.
2. Minimum password change of character requirements as defined as above and are enforced when new passwords are created by using Azure Active Directory password protection GPOs.

**IA.L2-3.5.8 - Prohibiting password reuse for a specified number of generations:**

1. The number of generations during which a password cannot be reused is specified as 24.
2. Currently, the reuse of passwords is prohibited during the specified number of generations (24) and depicted in password GPOs of the company GCC-H Enclave and mobile device management. It is the responsibility of the <role> to ensure that no deviations are made to this Group Policy configuration.

**IA.L2-3.5.9 - Allowing temporary password use for system logons with an immediate change to a permanent password:**

1. Once a user or administrator account is created, the user or administrator is assigned a temporary password that is provided by the [COMPANY NAME] IT Department. The user or administrator must change his temporary password immediately upon their first login. Account provisioning and temporary password creation is a part of the onboarding process for employees at [COMPANY NAME]. [COMPANY NAME] requires that initial passwords for information systems, such as an initial administrator password, be changed promptly upon information system installation.

**IA.L2-3.5.10 - Storage and transmission of only cryptographically-protected passwords:**

1. All passwords are cryptographically protected as one-way hashes using Microsoft password hashing algorithms, for the storage of passwords. All passwords are stored in a non-reversible encryption.
2. All passwords are cryptographically protected as one-way hashes Microsoft password hashing algorithms, for the transmission of passwords. All passwords are stored in a non-reversible encryption.

**IA.L2-3.5.11 – Obscuring feedback of authentication information during the authentication process:**

1. The Information System components are configured to obscure feedback of authentication information (displaying asterisks or bullet symbols when typing passwords) during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**Roles and Responsibilities**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |

# Non-Compliance

Violations of this Procedure will be treated like other allegations of wrongdoing at [COMPANY NAME]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 12/7/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |