Identity and Access Management Policy

Regular and Privileged Accounts

SA

Secured approach  www.securedapproach.com

Use Disclaimer: This policy has been developed by Secured Approach Inc. for the benefit of the community. You are welcome to use this policy, in whole or in part, for your organization without the need for prior approval. Should you wish to contribute to creating or updating a new version of this policy, please reach out to us via email at resources@securedapproach.com.
Furthermore, if you require assistance in crafting a tailored security policy for your specific environment, do not hesitate to contact us at support@securedapproach.com.

Table of Contents

[Confidentiality Statement 2](#_Toc159342162)

[Disclaimer 2](#_Toc159342163)

[1. Overview 2](#_Toc159342164)

[2. Purpose 2](#_Toc159342165)

[3. Scope 2](#_Toc159342166)

[4. Policy 3](#_Toc159342167)

[4.1 Password Protection 3](#_Toc159342168)

[4.2 Account Protection 3](#_Toc159342169)

[5. Policy Compliance 3](#_Toc159342170)

[5.1 Compliance Measurement 3](#_Toc159342171)

[5.2 Exceptions 4](#_Toc159342172)

[5.3 Non-Compliance 4](#_Toc159342173)

[6. Related Standards, Policies, and Processes 4](#_Toc159342174)

[7. Revision History 4](#_Toc159342175)

# Confidentiality Statement

This document is proprietary and confidential. It is intended solely for the use of [Organization Name] and its employees. Unauthorized distribution, copying, or use of this document or the information contained within is strictly prohibited and may be subject to penalties.

# Disclaimer

This Identity and Access Management Policy is subject to change at any time without notice. Regular updates may occur to comply with new regulations, technologies, and organizational needs. Users are responsible for staying informed about policy updates.

# Overview

The Identity and Access Management (IAM) Policy of [Organization Name] establishes the standards for managing user identities and controlling access to company resources. It aims to ensure secure and efficient access management across all systems and applications.

# Purpose

The purpose of this policy is to minimize security risks associated with digital identity management and access control. It seeks to protect sensitive information from unauthorized access while maintaining user accessibility necessary for operational efficiency.

# Scope

This policy applies to all employees, contractors, and third-party users of [Organization Name] who access organizational information systems. It encompasses all systems, applications, and data for which [Organization Name] is responsible.

# Policy

## Password Protection

* **Password Creation Guidelines:** Users must create strong passwords with a minimum of 12 characters, including uppercase and lowercase letters, numbers, and symbols.
* **Password Creation Guidelines:** Passwords should be random, unique, and complex, adhering to the organization's password creation guidelines.
* **No password re-use:** Passwords for Organization’s systems must not be used for other accounts or platforms.
* **Resetting Passwords:** Passwords must be reset immediately after any potential security compromise.
* **Password Managers:** The use of password managers is encouraged to securely store and manage passwords.
* **Privileged Accounts:** Stronger and longer passwords are required for privileged and administrative accounts, with regular review and updates.

## Account Protection

* **Separation of Work and Personal Accounts:** Work accounts should not be used for personal purposes and vice versa, to prevent security breaches and data leakage.
* **Multi-Factor Authentication (MFA):** MFA must be used for accessing sensitive systems and information where possible.
* **No Account Info Sharing:** Sharing account credentials is strictly prohibited. Each user must have individual access credentials.

# Policy Compliance

## Compliance Measurement

Compliance with this policy will be regularly monitored through audits, access reviews, and system logs analysis.

## Exceptions

Any exceptions to this policy due to compatibility issues or limitations must be submitted in writing with a business justification and approved by the IT Security Department or relevant authority within the organization.

## Non-Compliance

Violations of this policy may result in disciplinary action, up to and including termination of employment, legal action, and financial liability.

# Related Standards, Policies, and Processes

* Acceptable Use Policy
* Data Protection Policy
* Remote Access Policy
* Security Awareness Training Policy

# Revision History

This policy will be reviewed and updated annually or as needed to reflect changes in technology, legal requirements, and organizational priorities. The revision history will be documented here, including the date of the revision, a brief description of the changes, and the version number.

|  |  |  |  |
| --- | --- | --- | --- |
| Date of Change | Responsible | Summary of Change | Version |
| January 2024 | Information Security Manager | Building the first draft | 1.0 |
| January 2024 |  |  |  |
|  |  |  |  |