****

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.

Acceptable Use Policy

Internet and Technology

SA

Secured approach  www.securedapproach.com

Table of Contents

[Confidentiality Statement 2](#_Toc159258030)

[Disclaimer 2](#_Toc159258031)

[1. Overview 2](#_Toc159258032)

[2. Purpose 2](#_Toc159258033)

[3. Scope 2](#_Toc159258034)

[4. Policy 3](#_Toc159258035)

[4.1 Acceptable Use 3](#_Toc159258036)

[4.2 Security and Confidentiality 3](#_Toc159258037)

[4.3 Prohibited Activities 3](#_Toc159258038)

[5. Policy Compliance 3](#_Toc159258039)

[5.1 Compliance Measurement 3](#_Toc159258040)

[5.2 Exceptions 4](#_Toc159258041)

[5.3 Non-Compliance 4](#_Toc159258042)

[6. Related Standards, Policies, and Processes 4](#_Toc159258043)

[7. Revision History 4](#_Toc159258044)

# Confidentiality Statement

This document contains sensitive and confidential information pertaining to the organization's operational practices. The dissemination, distribution, or copying of this policy outside of the organization without explicit authorization is strictly prohibited. Access to this policy is limited to individuals who agree to maintain its confidentiality and are authorized by the organization. Violation of this confidentiality statement may result in disciplinary action, up to and including termination of employment and legal action.

# Disclaimer

This Acceptable Use Policy (AUP) may be updated periodically to reflect the evolving nature of technology and the internet. It is the responsibility of all users to stay informed about the policy updates. The organization reserves the right to amend this policy at any time.

# Overview

The Acceptable Use Policy (AUP) defines the guidelines and acceptable practices for the use of the organization’s internet and technology resources. This policy aims to ensure that these resources are used for purposes that are appropriate, ethical, and lawful.

# Purpose

The purpose of this AUP is to protect the organization's technological assets, reputation, and legal standing by preventing the misuse of its internet and technology resources. This policy outlines the acceptable use of these resources to ensure they contribute positively to the organization's goals and operations.

# Scope

This policy applies to all employees, contractors, and any individuals who have access to the organization's technology resources, including but not limited to computers, mobile devices, network resources, and internet services.

# Policy

## Acceptable Use

* Users must respect the integrity of computing systems; for example, users should not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
* Internet and technology resources should only be used for legitimate business purposes in accordance with the organization's objectives.
* Users must not access, distribute, or store any information that is illegal, offensive, or violates the rights of others.

## Security and Confidentiality

* Users are responsible for the security of their devices and data. This includes using strong passwords and not sharing account information.
* Confidential information must not be disclosed without authorization and must be protected according to the organization's data protection policies.

## Prohibited Activities

* Installing unauthorized software or hardware.
* Engaging in activities that can harm the organization’s network or devices, such as downloading or distributing potentially unwanted programs or malicious software.
* Using the organization’s resources for personal gain or illegal activities.

# Policy Compliance

## Compliance Measurement

The IT department will regularly audit and monitor the use of technology resources to ensure compliance with this policy. This may include, but is not limited to, network traffic monitoring and access logs.

## 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 will result in disciplinary action, which may include termination, legal action, and financial liability.

# Related Standards, Policies, and Processes

* Data Protection Policy
* Security Awareness Policy
* Remote Access 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 |  |  |  |
|  |  |  |  |