Security Baseline Policy

Foundational Security Measures

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](mailto: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](mailto:support@securedapproach.com).

Table of Contents

[Confidentiality Statement 2](#_Toc159342249)

[Disclaimer 2](#_Toc159342250)

[1. Overview 2](#_Toc159342251)

[2. Purpose 2](#_Toc159342252)

[3. Scope 2](#_Toc159342253)

[4. Policy 3](#_Toc159342254)

[4.1 Password Protection and Creation 3](#_Toc159342255)

[4.2 Data Protection Guidelines 3](#_Toc159342256)

[4.3 Security Awareness Participation 3](#_Toc159342257)

[4.4 Secure Configuration and Technology Protection 3](#_Toc159342258)

[4.5 Network Security 3](#_Toc159342259)

[4.6 Physical Security 3](#_Toc159342260)

[4.7 Incident Response 4](#_Toc159342261)

[5. Policy Compliance 4](#_Toc159342262)

[5.1 Compliance Measurement 4](#_Toc159342263)

[5.2 Exceptions 4](#_Toc159342264)

[5.3 Non-Compliance 4](#_Toc159342265)

[6. Related Standards, Policies, and Processes 4](#_Toc159342266)

[7. Revision History 5](#_Toc159342267)

# Confidentiality Statement

This document contains sensitive information intended solely for the use of [Organization Name]'s employees and authorized personnel. Unauthorized distribution, copying, or disclosure of this document, or the information contained within, is strictly prohibited and may lead to disciplinary actions.

# Disclaimer

This Security Baseline Policy is subject to change and may be updated periodically to reflect new security practices, compliance requirements, and technological advancements. It is the responsibility of all employees and stakeholders to stay informed of these changes.

# Overview

The Security Baseline Policy defines the minimum security standards that [Organization Name] requires to protect its information assets and technology infrastructure from potential threats and vulnerabilities.

# Purpose

To establish a foundation of security practices and measures that all users and business units must adhere to, in order to ensure the confidentiality, integrity, and availability of [Organization Name]'s data and systems.

# Scope

This policy applies to all employees, contractors, and third-party service providers of [Organization Name] who have access to the organization's information systems, data, and network.

# Policy

## Password Protection and Creation

* All users must follow [Organization Name]'s password protection and creation guidelines, including the use of strong, unique and complex passwords and no password re-use.

## Data Protection Guidelines

* Users must adhere to data protection guidelines to safeguard sensitive and confidential information from unauthorized access, disclosure, alteration, or destruction.

## Security Awareness Participation

* All users are required to participate in security awareness training programs to stay informed about current cybersecurity threats, best practices, and the organization's security policies.

## Secure Configuration and Technology Protection

* Users must ensure that their devices are configured securely and protected by up-to-date anti-malware software. This includes the regular application of patches and updates to operating systems and applications.

## Network Security

* Implement and maintain appropriate measures to secure the network infrastructure, including the use of firewalls, intrusion detection systems, and secure VPNs for remote access.

## Physical Security

* Secure physical access to [Organization Name]'s facilities and equipment to prevent unauthorized access, theft, or damage.

## Incident Response

* Follow [Organization Name]'s incident response procedures in the event of a security breach or incident.

# Policy Compliance

## Compliance Measurement

Compliance with this policy will be regularly audited and monitored through security assessments, system audits, and review of access controls.

## 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 access, employment, legal action, and financial liabilities.

Non-compliance by a Third-Party with the provisions of this policy may result in termination of the relationship, along with potential legal and financial repercussions.

# Related Standards, Policies, and Processes

* Acceptable Use Policy
* Identity and Access Management Policy
* Remote Access Policy
* Data Protection Policy
* Security Awareness Policy
* Clean Desk Policy
* Third-Party Management 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 |  |  |  |
|  |  |  |  |