Data Protection Policy

Data Protection Requirements

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](#_Toc159342141)

[Disclaimer 2](#_Toc159342142)

[1. Overview 2](#_Toc159342143)

[2. Purpose 2](#_Toc159342144)

[3. Scope 2](#_Toc159342145)

[4. Policy 2](#_Toc159342146)

[4.1 Data Handling 2](#_Toc159342147)

[4.2 Data Backup 3](#_Toc159342148)

[4.3 Data Disposal 3](#_Toc159342149)

[4.4 Data Breach Response 3](#_Toc159342150)

[4.5 Training and Awareness 3](#_Toc159342151)

[4.6 Monitoring and Logging 3](#_Toc159342152)

[5. Policy Compliance 3](#_Toc159342153)

[5.1 Compliance Measurement 3](#_Toc159342154)

[5.2 Exceptions 4](#_Toc159342155)

[5.3 Non-Compliance 4](#_Toc159342156)

[6. Related Standards, Policies, and Processes 4](#_Toc159342157)

[7. Revision History 4](#_Toc159342158)

# Confidentiality Statement

This document contains confidential information intended solely for the use of [Organization Name]'s employees and authorized individuals. Unauthorized distribution, reproduction, or disclosure of this document or any information contained within it is strictly prohibited and may result in disciplinary action.

# Disclaimer

This Data Protection Policy is subject to change to adapt to new regulations, technologies, and organizational practices. It is the responsibility of all stakeholders to stay informed of these updates.

# Overview

The Data Protection Policy of [Organization Name] sets forth the principles and standards for safeguarding the confidentiality, integrity, and availability of the organization’s data across all mediums.

# Purpose

To ensure that all employees and authorized users understand their responsibilities in protecting the data assets of [Organization Name] from unauthorized access, disclosure, alteration, destruction, or misuse.

# Scope

This policy applies to all employees, contractors, and third-party service providers of [Organization Name] who have access to data managed by the organization, regardless of the data format or where the data is stored.

# Policy

## Data Handling

* Data must not be shared with external parties without explicit approval from the designated authority within the organization.
* Copying or storing organizational data on personal devices is strictly prohibited unless specifically allowed and secured by IT-approved encryption tools.
* Access to data should be limited to only those individuals who require it to perform their job duties.
* Encryption mechanisms must be used while storing and transmitting data to ensure its confidentiality and integrity.

## Data Backup

* Regular backups of critical data must be performed to ensure its recoverability in case of data loss or corruption.

## Data Disposal

* Data that is no longer needed or has met its retention period must be disposed of securely and in accordance with regulatory requirements.

## Data Breach Response

* In the event of a data breach, follow the predefined incident response plan to mitigate risks and comply with legal and regulatory obligations.

## Training and Awareness

* All users must receive regular training on data protection practices, including understanding this policy and its importance.

## Monitoring and Logging

# Policy Compliance

## Compliance Measurement

Compliance with this policy will be regularly audited through internal reviews, audits, and monitoring of data handling practices.

## 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.

# Related Standards, Policies, and Processes

* Acceptable Use Policy
* Identity and Access Management Policy
* Remote Access Policy
* Security Awareness Policy
* Data Backup 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 |  |  |  |
|  |  |  |  |