Clean Desk Policy

Workplace 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](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](#_Toc159342096)

[Disclaimer 2](#_Toc159342097)

[1. Overview 2](#_Toc159342098)

[2. Purpose 2](#_Toc159342099)

[3. Scope 2](#_Toc159342100)

[4. Policy 2](#_Toc159342101)

[4.1 Workspace Requirements 2](#_Toc159342102)

[5. Policy Compliance 3](#_Toc159342103)

[5.1 Compliance Measurement 3](#_Toc159342104)

[5.2 Exceptions 3](#_Toc159342105)

[5.3 Non-Compliance 3](#_Toc159342106)

[6. Related Standards, Policies, and Processes 3](#_Toc159342107)

[7. Revision History 4](#_Toc159342108)

# Confidentiality Statement

This document contains proprietary information intended only for the employees and authorized personnel of [Organization Name]. Unauthorized sharing, copying, or disclosure of any part of this document or its contents is strictly prohibited and may result in disciplinary action.

# Disclaimer

This Clean Desk Policy is subject to change and may be updated periodically to reflect new security practices, compliance requirements, and operational needs. It is the responsibility of all staff to stay informed of these changes.

# Overview

The Clean Desk Policy of [Organization Name] outlines the required practices for maintaining a clean, organized, and secure working environment, whether at the office, home office, boardrooms, or shared workspaces.

# Purpose

To minimize the risk of unauthorized access, information theft, and security breaches by ensuring that sensitive and confidential information is not left unattended on desks or within an easy reach of unauthorized individuals.

# Scope

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

# Policy

## Workspace Requirements

* All users must complete the mandatory security awareness training upon induction and participate in annual refresher courses.
* All confidential and sensitive documents must be secured in locked drawers or cabinets when not in use or when the workstation is unattended.
* Employees are required to clear their desks at the end of each workday, ensuring that all documents, notes, and removable storage devices are secured.
* In shared workspaces and boardrooms, users must ensure that all sensitive materials are collected and secured at the end of each meeting or work session.
* Confidential documents must be shredded or placed in secure disposal bins, not in regular trash cans.
* Employees working remotely must adhere to the same clean desk principles as in the office, ensuring that sensitive information is protected from family members or visitors.
* Laptops, tablets, and other electronic devices must be password-protected and locked or stored securely when not in use.

# Policy Compliance

## Compliance Measurement

Regular audits and spot checks will be conducted to ensure adherence to the Clean Desk Policy. This may include physical inspections or review of security camera footage.

## Exceptions

Any exceptions to this policy 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
* Data Protection Policy
* Security Awareness 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 |  |  |  |
|  |  |  |  |