Clear Desk Policy

Last updated: November 2023

1. Overview

To improve the security and confidentiality of information, Cloudoko has adopted a Clear Desk Policy for computer and printer workstations.

This ensures that all sensitive and confidential information is properly locked away or disposed of when a workstation is not in use. This includes whether the information is on:

- paper
- storage device
- hardware device

2. Purpose

The Clear Desk Policy will reduce the risk of unauthorised access. This includes the loss of, and damage to, information during and outside of normal business hours, or when workstations are left unattended.

A Clear Desk Policy is an important security and privacy control.

3. Scope

This policy applies to all permanent, voluntary and contracted staff working directly or indirectly for Cloudoko.

4. Policy

Whenever a desk is unoccupied for an extended period of time the following will apply:

1. All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices, such as USB drives.
2. All waste paper that contains sensitive or confidential information must be shredded.
3. Computers must be locked when the desk is unoccupied and shut down at the end of the working day.
4. Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
5. Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
6. Printers and fax machines should be treated with the same care under this policy. This means:
    - any print jobs containing sensitive and confidential paperwork should be retrieved immediately – the 'locked print' functionality should be used
    - all paperwork left over at the end of the working day will be properly disposed of

5. Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including random and scheduled inspections.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

- None.

8. Revision History

Date of Change	Responsible	Summary of Change
November 2023	Kevin Boldy	Initial Version

www.cloudoko.com