Clean Desk Policy

1. Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of sight. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

3. Scope

This policy applies to all SproutLoud Media Networks employees.

4. Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.2 Computer workstations must be locked when the workspace is unoccupied.

4.3 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

4.4 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.5 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

4.6 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

4.7 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

4.8 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

4.9 Whiteboards containing Restricted and/or Sensitive information should be erased.

4.10 Lock away portable computing devices such as laptops and tablets.

4.11 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5. Remote Work

SproutLoud operates in a distributed work environment. Team members have been permitted to work from home on a full-time basis. In adherence to SproutLoud Remote Workplace Guidelines and Agreements and to ensure that employees' performance will not suffer in remote work arrangements, we advise our remote employees to:

a. Choose a quiet and distraction-free working space.
b. Have an internet connection that's adequate for their job.
c. Dedicate full attention to their job duties during working hours.
d. Adhere to break and attendance schedules agreed upon with their manager.
e. Employees should maintain a clutter-free and secure digital workspace. This includes organizing digital files, securely storing sensitive information, and ensuring that screen displays do not expose confidential data when left unattended.
f. For temporary working places (while traveling or out of the usual working space) adhere to the points listed in section 4.

6. Policy Compliance

6.1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

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

6.3 Non-Compliance

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

7 Related Standards, Policies and Processes

None.

8 Definitions and Terms

None.

9 Revision History

Date of Change	Responsible	Summary of Change	Version ID
12/2017	James Aggrey	Initial Release	1.0
4/2022	Gustavo Malpica	No Changes	1.0
3/2023	Gustavo Malpica	Added Remote Work Section	1.1
4/2024	Gustavo Malpica	Added Section 5.e	1.2