Clean Desk Policy

1. Overview

Sensitive documents and materials are liable to intentional or unintentional disclosure to unauthorised parties when they become unaccounted for. A Clean Desk Policy is a useful tool for helping ensure that sensitive and confidential material does not go unaccounted for or become exposed. A Clean Desk Policy in its most basic form requires employees to completely clear their desks at the end of their workday, moving items to drawers and disposing of documents that are no longer needed. This protects Company data from unauthorised access as it reduces the number of sensitive data that is available to an unauthorised person who may gain access to the Company's premises.

2. Purpose

The purpose of this policy is to establish a clear procedure and minimum requirement for maintaining a Clean Desk. It details why a Clean Desk is important for data security, as well as the methods in which this is best achieved.

3. Scope

This policy applies to all employees, contractors, temporary workers and any other personnel that may work on behalf of the company or within the company's premises.

4. Policy

4.1. All sensitive, confidential or personal information in paper or electronic form must be secured at the end of the work day, or at any time when they are not in active use.
4.2. Keys to file cabinets or other secure storage spaces must not be left on desks or in other insecure areas.
4.3. Computers must be locked at any time when they are not in active use.
4.4. Computers must be shut down at the end of the work day.
4.5. Laptops must be locked in secure drawers or secured with a locking cable.
4.6. Printed material must be removed from the printer tray without undue delay and not be left around the printing area.
4.7. When no longer needed, documents containing confidential, sensitive or personal information must be shredded or inserted into confidential disposal bins.
4.8. Whiteboards must be erased after meetings or when no longer in use.

5. Compliance

5.1. Compliance Measurement

The Infosec team will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. Exceptions

Any exceptions to this policy must be approved by the Infosec team in advance and have a written record.

5.3. Non-Compliance

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