**CLEAN DESK POLICY**

|  |  |
| --- | --- |
| **Effective Date**  |  |
| **Reviewed by** |  |
| **Next scheduled review date**  |  |
| **Supersedes**  | All previous similar policies  |
| **Approved by**  |  |
| **Date approved** |  |

**1.1 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 site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

A clean desk policy can be an import 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

**1.2 Scope**

This policy applies to all employees and contractors including:

* Full time
* Part time
* Casuals
* Holders of a s.457 Visa
* Affiliates

In implementing this policy, the Employer will act in accordance with the requirements specified under relevant Awards, industrial agreements or legislation, and in a fair and equitable manner.

Employees are to act in accordance with this policy

**2.1 Clean Desk Policy**

* 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.
* Computer workstations must be locked when workspace is unoccupied.
* Computer workstations must be shut completely down at the end of the workday.
* 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 workday.
* File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
* Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
* Laptops must be either locked with a locking cable or locked away in a drawer.
* 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.
* Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
* Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
* Whiteboards containing Restricted and/or Sensitive information should be erased.
* Lock away portable computing devices such as laptops and tablets.
* 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.

**3.0 Policy Compliance**

**3.1 Compliance Measurement**

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

**3.2 Exceptions**

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

**3.3 Non-Compliance**

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

Please note Cyber Awareness Training is Recommended for all staff:



<https://the-answer-is-yes.teachable.com/p/cyber-essentials-for-all-staff>