**Clean Desk Policy**

**Overview**

Clean desk policy is placed to secure the physical security at HiQuSystems. The policy ensures the confidential information and sensitive materials are stored away and out of sight when custodian of the material is not in the premises/workplace.

The policy is set in place to keep the clean workspace, where confidential and sensitive material about company, clients, vendors, employees, and intellectual property is safe and secured.

The policy applies to employees, contractors, part time employees or any other individual engaged to perform any task for the company.

**Policy**

1. Employees are required to secure all sensitive/classified information in their workspace at the completion of the workday and when they are expected to be away from their workspace for an extended or short period of time. This includes both electronic and physical hardcopy information.
2. The Windows lock shall be password protected for reactivation
3. Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the workday. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.
4. Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.
5. Printed materials must be immediately removed from printers. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.
6. All sensitive documents and restricted information must be placed in the designated shredder bins for destruction, or placed in the locked confidential disposal bins.
7. File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.
8. Passwords must not be written down or stored anywhere in the office.
9. Keys and physical access cards must not be left unattended anywhere in the office.
10. The reception desk can be particularly vulnerable to visitors. This area shall be kept as clear as possible at all times.
11. Individual Personal belongings like bags, books, edibles, etc. shall be kept in drawers.
12. Company provided laptop/tablets/mobile phone should strictly be used for company purpose when working from home. The devices must not be shared with anyone not related to HiQuSystems directly or indirectly.
13. When working from home, the same rules applies to the sensitive and confidential information as of working in office.
14. Server rooms and office areas shall remain locked when they are not in use
15. File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended.
16. Keys used to access Confidential or Internal Use information must not be left in an unattended work area.
17. Passwords must not be posted on or under a computer or in any other accessible location.

It is the responsibility of each manager, supervisor or lead to ensure enforcement with the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions in accordance with company’s Employee Handbook.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, please notify your manager, supervisor, or lead **immediately.**

It’s a good practice to send an email to employees at the end of the day as a reminder to follow the policy guidelines.