[COMPANY NAME]
[Add your company logo / letterhead and registered address here]

Clear Desk and Clear Screen Policy

HOW TO USE THIS TEMPLATE
This template is mostly complete and pre-filled with standard Indian practice. You should not have to fill many blanks.
Text in blue is a default that companies commonly change. Skim the blue text and edit only what differs for you.
Add your company name and letterhead once, in the header above. The body refers to "the Company".
Pair this policy with a desk audit checklist and configure the auto-lock timeout centrally through Group Policy or MDM so the [[5 minute]] screen lock is enforced, not left to individual users.
Have it reviewed by a qualified HR or legal professional before you adopt it, and delete this box.
Provided by CFOmatrix (cfomatrix.in). General template, not legal advice.

Policy owner	**[Human Resources / IT / Compliance]**
Effective date	**[DD MMM YYYY]**
Version	1.0
Approved by	**[Name, Title]**

1. Purpose

This policy sets the standard for how employees and other authorised users keep their physical work areas and computer screens clear of sensitive material. Its objectives are:

- To reduce the risk of unauthorised access, loss, damage or theft of information, whether held on paper, on removable media or on screen.
- To protect confidential, personal and business critical information when a workspace is unattended or at the end of the working day.
- To support the Company's obligations under the Digital Personal Data Protection Act, 2023 (DPDP Act) to protect personal data through appropriate security safeguards, and to limit access to data on a need to know basis.
- To support the Company's information security framework and its alignment with recognised controls such as ISO 27001 (Annex A clean desk and clear screen controls) and SOC 2.

A clear desk and clear screen discipline is one of the simplest and most effective controls available, because most opportunistic information loss happens through documents left visible, screens left unlocked and media left unattended.

2. Scope

This policy applies to:

- All employees of the Company, whether permanent, probationary, fixed term or part time.
- Contractors, consultants, interns, trainees and temporary staff.

- Third party personnel, vendors and visitors who are present at any Company premises or who access Company information.

It covers all locations where Company information is handled, including:

- Company offices, meeting rooms, reception areas and shared spaces.
- Home offices and other remote or hybrid work locations.
- Co-working spaces, client sites and travel locations.

It covers information in all forms, including printed documents, handwritten notes, whiteboards, removable media (USB drives, external disks, memory cards), laptops, desktops, mobile devices, and any screen that may display Company or personal data.

3. Definitions

- Clear Desk: the practice of keeping the work surface free of papers, media and devices that contain sensitive information whenever the desk is unattended or at the end of the day.
- Clear Screen: the practice of ensuring that no sensitive information is left visible on any unattended screen, by locking or logging off.
- Sensitive Information: any information classified as Confidential, Restricted or Internal under the Company's data classification scheme, and all personal data of employees, customers or other individuals.
- Removable Media: any portable storage device, including USB flash drives, external hard drives, memory cards, optical media and portable SSDs.
- Confidential Waste: any document or media containing sensitive information that is no longer required and must be securely destroyed rather than placed in ordinary waste.

4. Information Classification Reference

Handling under this policy follows the Company data classification levels. Apply the strictest level present on the desk or screen.

Classification	Examples	Clear Desk and Screen Requirement
Restricted	Customer financial data, personal data, contracts, credentials, board papers	Never left unattended; locked in **a lockable drawer or cabinet**; screen locked on every absence
Confidential	Internal financials, HR records, strategy, source code printouts	Stored out of sight when unattended; cleared at end of day
Internal	Process notes, internal memos, non public project material	Not left visible to visitors; tidied at end of day
Public	Published marketing material, public website content	No special handling required

5. Clear Screen Requirements

All users must ensure that no sensitive information is left visible on an unattended screen.

- Lock the screen every time you leave your workstation, even for a short break. On Windows use Win + L; on macOS use Control + Command + Q; on Linux use the equivalent shortcut.
- Devices must be configured to lock automatically after **5 minutes** of inactivity, requiring a password, PIN or biometric to unlock. This timeout is enforced centrally through Group Policy or mobile device management (MDM) and must not be disabled or extended by the user.
- Log off or shut down devices at the end of the working day unless a system requires them to remain on for **overnight backups or updates**.
- Position screens so that sensitive information is not visible to passers by, visitors or through windows. Use a privacy screen filter when working in public spaces, on client sites or while travelling.
- Do not leave sensitive applications, dashboards, customer records or email open and visible during screen sharing, video calls or presentations; share only the specific window required.
- Never write down passwords on sticky notes, under keyboards or in visible locations. Use the approved password manager, **1Password / Bitwarden**.
- Mobile phones and tablets used for Company work must have a screen lock with auto-lock of **1 minute** or less and must require a PIN, password or biometric.

6. Clear Desk Requirements

When a desk is unattended for an extended period and at the end of each working day, the work surface must be clear of sensitive material.

- Documents containing Confidential or Restricted information must be locked in a **lockable drawer, pedestal or cabinet** when not in active use and at the end of the day.
- Do not leave files, notebooks, diaries or printed reports containing sensitive information open and visible on the desk.
- Keys to lockable furniture must not be left in the lock or on the desk; store them in **an assigned secure location**.
- Laptops and portable devices must be either taken with the user or secured with a cable lock or locked in a cabinet when left at the office.
- Reception desks, meeting rooms and shared hot desks must be cleared by each user after use; nothing sensitive may be left for the next occupant.
- Incoming and outgoing post containing sensitive information must not be left unattended in open trays.

7. Removable Media and Portable Devices

- The use of removable media is **restricted and discouraged**; use approved Company cloud storage and collaboration tools, **Google Drive / SharePoint**, in preference.
- Where removable media is permitted, it must be **encrypted** and must be locked away when not in use, never left in a drive or on the desk.
- Removable media containing sensitive information must not be taken off Company premises without authorisation from **the line manager or IT Security**.
- Lost or stolen media or devices must be reported immediately to **ITsecurity@company.com** so that data exposure can be assessed under the breach process in Section 12.
- Personal removable media must not be connected to Company devices unless expressly approved.

8. Printers, Copiers, Scanners and Fax

- Do not send sensitive documents to a printer and leave them in the output tray. Use secure or pull printing where available, releasing the job at the device with a PIN or badge.
- Collect printed, copied and scanned documents immediately. Documents left at shared devices for more than **15 minutes** should be treated as confidential waste and securely destroyed.
- Check the device glass and document feeder for originals after copying or scanning.
- Configure multifunction devices to clear stored job data and to require authentication for stored or held jobs.
- Do not print sensitive material to printers in unsecured or public areas.

9. Whiteboards, Flip Charts and Meeting Rooms

- Erase whiteboards and remove or shred flip chart pages that contain sensitive information at the end of every meeting.
- Do not leave meeting notes, printouts or named place cards behind in meeting rooms.
- When using glass walls or whiteboards visible from corridors or other rooms, avoid writing Restricted information, or position the board out of external sightlines.
- The last person to leave a meeting room is responsible for clearing it; book the room for a short buffer if clearing will take time.
- Disconnect from screen sharing and clear any displayed content on room screens before leaving.

10. End of Day and Extended Absence Routine

Before leaving at the end of the working day, or before any extended absence such as leave or travel, each user must complete the following checklist.

Step	Action	Done
1	Lock or shut down all computers and devices	[ ]

2	Clear the desk of all Confidential and Restricted documents	[ ]
3	Lock documents and removable media in a secure drawer or cabinet	[ ]
4	Collect any documents from printers, copiers and scanners	[ ]
5	Erase whiteboards and clear meeting rooms used	[ ]
6	Secure keys, access cards and tokens	[ ]
7	Place confidential waste in the designated secure bin	[ ]

For remote and hybrid workers, the same routine applies at the home workspace: lock devices, store papers out of sight from other household members and visitors, and do not leave sensitive material on shared dining or living surfaces.

11. Confidential Waste and Disposal

- Documents containing sensitive information must never be placed in ordinary waste or open recycling bins.
- Place such documents in the designated **locked confidential waste bin or shredder** for secure destruction by **the approved disposal vendor**.
- Cross cut shredding (or finer) is the minimum standard for on site shredding of paper.
- Removable media and storage devices that are being retired must be securely wiped or physically destroyed by **IT**; they must not be discarded intact or donated without sanitisation.
- A certificate of destruction should be obtained from any third party disposal vendor and retained by **IT / Admin**.
- Disposal of records must respect applicable retention requirements; do not destroy records that are subject to a legal hold or a statutory retention period.

12. Incident Reporting

- Any actual or suspected breach of this policy, including documents left exposed, an unlocked unattended screen accessed by an unauthorised person, or lost media, must be reported promptly to **ITsecurity@company.com** or **the line manager**.
- Where the incident may involve loss of or unauthorised access to personal data, the Company's data breach process under the DPDP Act applies, including assessment of the breach and, where required, notification to the Data Protection Board of India and to affected data principals.
- Where the incident is a reportable cyber security incident, the Company must report to CERT-In within 6 hours of becoming aware of it, in line with the CERT-In Directions, 2022.

- Do not attempt to conceal or quietly remedy an incident; prompt reporting reduces harm and is treated more favourably than non disclosure.

13. Roles and Responsibilities

- All Users: comply with this policy at all times, lock screens, clear desks and report incidents.
- Line Managers: set the example, conduct or support periodic desk checks for their teams, and address non compliance.
- IT / Information Security: configure and enforce the auto-lock timeout and encryption, provide secure printing and approved storage, sanitise retired media, and investigate incidents.
- Facilities / Admin: provide lockable storage, confidential waste bins and shredding services, and manage the disposal vendor.
- Human Resources: incorporate this policy into onboarding, awareness training and the disciplinary process.
- **Chief Information Security Officer / IT Head**: owns this policy and its annual review.

14. Compliance Monitoring and Enforcement

- The Company may carry out periodic and unannounced clear desk and clear screen walkthroughs, including out of hours sweeps, to verify compliance.
- Findings are logged and shared with the relevant line manager; repeated or serious lapses are escalated.
- Unattended sensitive documents found during a sweep may be removed and secured by the auditor, with a note left for the user.
- Failure to comply with this policy may be treated as misconduct and may lead to disciplinary action up to and including termination of employment or contract, and may carry personal liability where it results in a breach of law.
- Contractors and third parties who breach this policy may have their access withdrawn and their engagement reviewed.

15. Review and Governance

This policy is owned by **IT Security / the Information Security function** and approved by **the Management / Board**. It will be reviewed at least once every **12 months**, or earlier following a significant incident, a material change in operations or premises, or a change in applicable law. Employees will be informed of material changes, and the latest version supersedes all previous versions.