|  |  |
| --- | --- |
| RECORD OF TOOL BOX TALK | |
| Workplace: | Date: |
| Name of supervisor or presenter: | Time: |
| Topics discussed: Accident / Incident / Illness Reporting | |
| **CLEAN DESK POLICY - CLIENT AND BUSINESS PRIVACY**  **What is a**[**Clean Desk Policy**](https://www.shredit.com.au/en-au/resource-center/fact-sheets/establishing-a-clean-desk-policy)**?**  It specifies how employees should keep their working space, and it’s one of the simplest ways to help comply with privacy laws, emphasise information security in the workplace, and reduce the risk of a data breach and [identity theft](https://www.shredit.com.au/en-au/resource-center).  Here is a checklist for keeping workspaces tidy – and secure.  **Start of the workday**   * Staff and others should plan work tasks when they arrive, gathering together only the documents and devices necessary to do the job. * After viewing emails and opening needed documents, reduce or close pages on the screen. * Try to always be aware of any confidential information being used. * Use a simple filing system so that documents are filed straight away. * A good [document management](https://www.shredit.com.au/en-au/resource-center/white-papers-case-studies/developing-a-document-management-policy) process also limits access to confidential data to those who need the information to do their jobs.   **Leaving the workspace temporarily**   * Do a quick scan of the work area and remove and secure any visible sensitive information. * Switch on the password-protected screen saver. * Take printed documents that are no longer needed and put them into locked consoles provided by a document destruction partner for [secure shredding](https://www.shredit.com.au/en-au/secure-shredding-services/paper-shredding-services). * Carry mobile devices or secure them inside a drawer.   **Other workday chores**   * As far as practicable, when sensitive or [confidential information](https://www.shredit.com.au/en-au/resource-center/fact-sheets/what-documents-to-shred) is being worked on, close or minimise the window or lock the computer when unauthorised persons are nearby. * Never leave confidential documents unattended on flip charts or whiteboards in meeting rooms. When the meeting is over, do not leave behind any confidential notes or information in plain view. * In shared printer areas, immediately remove all sensitive documents from equipment.   **End of the day**   * Clear desk of papers including sticky notes and papers that contain sensitive information. * Log out of desktop computer and shut it down. * Securely store removable computer devices, DVDs, USB sticks, etc. * Lock draws and filing cabinets, and store keys in a secure location. | |