



Policy Name:	Document Security & Clean Desk Policy
Attention:	LSH Group Australia Employees
Version:	1.3
Last Reviewed:	1 st April 2026
Effective From:	1 st April 2026
Approved By:	GCEO / Corp Review / MD

Document Security & Clean Desk Policy

1. Purpose

This policy outlines the requirements for secure handling of information and maintaining a clean desk environment to protect LSH Group Australia's information assets from unauthorised access, disclosure, misuse, loss, or damage.

This policy supports compliance with:

- *Privacy Act 1988 (Cth)* and *Australian Privacy Principles (APPs)*
- *Notifiable Data Breaches (NDB) Scheme*
- Applicable confidentiality and data protection obligations

2. Scope

This policy applies to all employees, contractors, temporary staff, and third parties who access or handle Company information, whether:

- On Company premises; or
- Working remotely or offsite

3. Policy Principles

All information must be:

- Protected in accordance with its level of sensitivity
- Accessible only to authorised personnel
- Stored, transmitted, and disposed of securely
- Handled in a way that minimises the risk of privacy breaches

4. Document Security

4.1 Information Classification

All information must be classified and handled appropriately:

- **Confidential** – Sensitive business or personal information (e.g. customer data, financial records)
- **Internal Use** – Information for internal business use only
- **Public** – Information approved for public release

4.2 Storage and Access

Employees must:



- Store confidential documents in locked cabinets or secure systems
- Restrict access to authorised personnel only
- Ensure electronic information is stored in approved Company systems
- Avoid storing Company information on personal devices unless authorised

4.3 Transmission of Information

Sensitive information must only be transmitted using secure methods, such as:

- Encrypted email or secure file transfer systems
- Approved Company platforms

Employees must take reasonable steps to verify recipients before sending information.

4.4 Printing and Physical Documents

- Printing of sensitive information should be limited to business necessity
- Printed documents must be collected immediately from printers
- Documents must not be left unattended in shared areas

4.5 Disposal of Information

- Paper records containing sensitive information must be disposed of using secure shredding
- Electronic records must be securely deleted in accordance with Company procedures
- Information must not be retained longer than necessary, subject to legal and business requirements

4.6 Customer and Personal Information

All customer and personal information must be handled in accordance with:

- Privacy obligations under the *Privacy Act 1988 (Cth)*
- Company Privacy Policy

Failure to secure personal information may constitute a notifiable data breach.

5. Clean Desk Requirements

Employees must maintain a clean and secure workspace, including:

- Removing and securely storing all confidential or sensitive documents when not in use
- Ensuring items such as:
 - Contracts, deal documents, loan agreements
 - Customer identification (e.g. licences)
 - Financial information (e.g. credit card details)
 - Notes, diaries, and business cardsare not left visible or unattended
- Clearing whiteboards and meeting areas of confidential information after use
- Securing keys, access cards, and other sensitive items
- Locking or logging off computers when unattended
- Securing laptops, mobile devices, USBs, and portable storage
- Avoiding discussions of confidential matters in public or shared spaces

6. Remote Work Requirements



When working remotely, employees must:

- Ensure documents and devices are not visible to unauthorised persons
- Use secure networks and approved systems
- Store physical documents securely and dispose of them appropriately
- Maintain the same level of confidentiality as in the workplace

7. Incident Reporting and Breaches

Employees must immediately report any:

- Lost or stolen documents or devices
- Unauthorised access or disclosure of information
- Suspected or actual data breaches

Reports must be made to the Manager, IT, or Human Resources.

All incidents will be assessed in accordance with the *Notifiable Data Breaches (NDB) Scheme*, and appropriate action will be taken.

8. Responsibilities

Employees

- Comply with this policy and handle information securely
- Maintain a clean and secure workspace
- Report any risks or breaches promptly

Managers

- Ensure team awareness and compliance
- Reinforce secure work practices

IT / Security / HR

- Provide secure systems, training, and support
- Monitor risks and investigate incidents
- Ensure compliance with legal obligations

9. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, and may expose individuals to legal liability.

All matters will be assessed on a case-by-case basis, considering the nature and impact of the breach.

10. Review

This policy will be reviewed periodically to ensure compliance with legislation and alignment with best practice.

8. Policy Status

This Policy does not form part of any employee's contract of employment. It is a lawful and reasonable direction of the Company with which compliance is required. Any statement in this



Policy about what the Company will or will not do does not create a legally binding obligation on the Company.

This Policy may be amended from time to time to reflect changes in legislation, regulatory requirements or organisational needs.