



**Legal Profession
Admission Board**
of New South Wales

Information Security Policy

About this policy

This policy outlines the Legal Profession Admission Board's (LPAB) framework for managing information security.

Purpose

1. The LPAB is the body that assesses candidates for admission as lawyers or for appointment as public notaries, accredits law schools and practical legal training providers, and conducts examinations that lead to the award of the Diploma in Law.
2. LPAB is committed to ensuring the confidentiality, integrity and availability of its client's information and the information of LPAB as a whole.
3. This policy sets out the framework for managing the security of LPAB's information systems by identifying roles, responsibilities and accountability of users.

Scope

4. This policy applies to:
 - Members of the Board, its Committees, and its Sub-Committees
 - Employees (ongoing, temporary, and casual)
 - Contractors
5. LPAB operates under a shared services agreement with DCJ. Information stored by DCJ under that agreement will be covered by the relevant DCJ policies in place from time to time. This policy applies in tandem with the DCJ Information Security Policy.

Definitions

6. In this policy:
 - **Board** means the governing body of the Legal Profession Admission Board of New South Wales.
 - **Committee** means a committee established under the NSW Admission Board Rules 2015.
 - **DCJ** means the Department of Communities and Justice
 - **Employee** means a person who is employed by LPAB and includes contractors and contingent labour workers.
 - **Executive Officer** means the person appointed as Executive Officer to the Board under the *NSW Admission Board Rules 2015*.
 - **LPAB** stands for the Legal Profession Admission Board, which is the corporation established under the *Legal Profession Uniform Law Application*

Act 2014.

- **Sub-Committee** means a sub-committee established under the *NSW Admission Board Rules 2015*.

Requirements

7. LPAB approach to information security is underpinned by:
 - Being accountable for the security and management of its information.
 - Implementing controls relative to the value and sensitivity of the information, commensurate with the risk of loss or compromise.
 - Information is accessed only by users with a need to know
 - Segregation of duties to reduce opportunities for unauthorized access.
8. It manages that responsibility in co-operation with DCJ through a shared services agreement.
9. LPAB data and information are stored on DCJ systems that are maintained and protected by DCJ. DCJ will manage the security of those information assets in accordance with its own policies and procedures. LPAB will support DCJ in undertaking those functions.
10. Some information cannot be stored in DCJ systems. Where that is necessary, the amount of information outside DCJ systems will be minimized. Where data and information cannot be stored on DCJ systems, the Executive Officer is responsible for managing that information.
11. The Executive Officer shall have overall administrative and operational responsibility for LPAB's information.
12. The Board and its committees, employees, and contractors all have a duty to follow relevant information security policies, processes and standards to ensure the protection of information assets.
13. The Executive Officer shall communicate to employees and contractors the ongoing responsibilities in relation to information security.
14. The Executive Officer shall report to the Board, identify any risks that the Board should include in the risk register, and otherwise exercise sound business judgment in protecting information.
15. Where a security incident occurs, the Executive Officer shall work with DCJ and appropriate law enforcement and regulatory bodies.

Related policies

16. This policy aligns with the LPAB Cyber Security Policy.

Review

17. This policy will be reviewed every three years from its last update to ensure that it remains current, effective, and aligned with organizational, legislative, and regulatory requirements.

Document information

Title:	Information Management Security Policy
Approver:	Legal Profession Admission Board
Date of Effect:	9 June 2026
Next review:	9 June 2029
File Reference:	CTSD26/750
Policy owner:	Executive Officer
Key Words:	Information security

Document history

Version	Date	Reason for Amendment
1.0	9/6/2026	Initial policy.

(End)