Legal Profession
Admission Board
of New South Wales

Cyber-Security Policy

Table of Contents

1 Purpose

Information security is fundamental to the successful operation of LPAB and it is committed to ensuring the integrity of its information systems. This policy establishes a framework for managing information security risks within LPAB. It is intended to bring LPAB's processes into alignment with each of the following:

- NSW Cyber policy and the
- DCJ Information and Security policy.

This policy will supplement those polices so that LPAB operations will:

- emphasize proactive identification and mitigation of security risks.
- define responsibilities for information security.
- provide for regular reviews and compliance checks.
- provide for security controls in case of incidents.

This policy applies to:

- LPAB
- Members of LPAB
- Members of the Committees and sub-committees of LPAB
- Third-party service providers engaged directly by LPAB
- Employees of the Board (including DCJ employees)

This policy does not apply to the Judiciary who are subject to the Judicial Protocol to Information Security.

This policy is intended to provide a supplementary framework to the Information and Security Policy[1] of the Department of Communities and Justice (DCJ).

[1] The DCJ policy is publicly available at:

https://dcj.nsw.gov.au/documents/resource-centre/policies/information-security-policy.pdf

2 Definitions

Board	comprises those persons who are nominated to LPAB
DCJ	is the Department of Communities and Justice
Executive Officer	is the person appointed by LPAB to that role, including any person acting in that role
LPAB	means the Legal Profession Admissions Board
Senior management team	means the management team reporting to the Executive Officer
Shared services	any agreement in place between LPAB and DCJ relating to provision of services to LPAB

3 Statement of alignment

LPAB has a shared services agreement with DCJ to provide the Information and Records management support for the Board. As a result, LPAB will adhere to and adopt the relevant policies that relate to Information Security published by DCJ from time to time, subject to any appropriate modifications. LPAB is committed to adopting and following those policies when using services provided by DCJ under shared services.

LPAB may from time to time engage services from vendors outside of those managed by DCJ. LPAB will apply the relevant DCJ policies and procedures as closely as possible and will seek advice from DCJ whenever possible in respect of those services before implementing them. Where DCJ cannot provide that advice, LPAB will undertake its own due diligence.

4 Incident Management

DCJ will have primary responsibility for cyber-security affecting systems hosted by DCJ. Incident management is a service provided under the shared services agreement.

LPAB will ensure that all cyber-security incidents will be reported immediately to the Cyber Security Team in DCJ. Contact with external authorities will be coordinated through designated personnel nominated by DCJ.

LPAB will maintain its own incident register and will record remediation actions in that register. It will make that register available to DCJ to enable DCJ to comply with any relevant obligation that it has in respect of cyber-security.

5 Monitoring and Auditing

LPAB provides a Cyber Security Annual Attestation Statement each financial year as part of its financial audit. The statement is required by the NSW Government Cyber Security Policy.

Separate to this Statement, LPAB will conduct its own periodic internal and external audits of its systems independently of DCJ as necessary. This will include:

- Periodic review of users who have access to LPAB information systems and ensure that access is based on least privilege
- Internal audits of processes of LPAB
- Audit of third-party vendors for risks

LPAB will report from time to time to its Audit and Risk Committee on its compliance with this policy.

6 Training and Awareness

LPAB will seek to ensure that members, committee members, contractors and staff who have access to LPAB systems have been or will be trained in cyber-security awareness.

LPAB will ensure that staff who access DCJ systems will have completed any required DCJ training for that system.

7 Responsibilities

LPAB has primary responsibility for implementing this policy. The Board will have responsibility for governance of the policy.

The Executive Officer will carry out, implement, and monitor this policy. The Executive Officer may allocate responsibility to the management team of LPAB for aspects of this plan.

All Board members, committee members and staff remain responsible for securing their own access to LPAB's systems.

8 Document information

Document name	LPAB Cyber-Security Policy
Document reference	CTSD25/1035
Replaces	None
Applies to	All LPAB
Policy administrator	Executive Officer
Approval	The Board of LPAB

9 Version and review details

Version	Effective date	Reason for amendment	Due for review
1.0	27 June 2025	Initial policy	1/7/2026